# Mes développements d'agrégation

Valentin Massicot

Janvier 2024 - Juin 2024

# Enveloppe convexe de $\mathrm{O}_n(\mathbb{R})$

## Cadre :

Soit $n \geqslant 2$. L'enveloppe convexe de $\mathrm{O}_n(\mathbb{R})$ dans $\mathrm{M}_n(\mathbb{R})$ est la boule unité fermée pour la norme subordonnée à la norme euclidienne de $\mathbb{R}^n$.

**Recasages** :

- 106 Groupes linéaires
- 158 Endomorphismes d'un espace euclidien
- 159 Formes linéaires et dualité
- 161 Espaces vectoriels et affines euclidiens
- 181 Convexité dans $\mathbb{R}^n$ en algèbre et géométrie
- 191 Techniques d'algèbres en géométrie

**Référence** : L3 algèbre Pearson.

## Développement :

**Soit $f \in \mathrm{M}_n(\mathbb{K})^*$, montrer il existe $A \in \mathrm{M}_n(\mathbb{K})$ telle que $f = \mathrm{Tr}(A\,\cdot\,)$ par analyse-synthèse.**

**Analyse** : supposons qu'il existe $A = (a_{ij})_{ij} \in \mathrm{M}_n(\mathbb{K})$ telle que $f(M) = \mathrm{Tr}(AM)$ pour tout $M \in M_n(\mathbb{K})$. Si $(E_{ij})_{ij}$ est la base usuelle de $\mathrm{M}_n(\mathbb{K})$, on a donc

$$\begin{aligned} f(E_{ij}) &= \mathrm{Tr}(AE_{ij}) \\ &= \sum_{kl} a_{kl}\,\mathrm{Tr}(E_{kl}E_{ij}) \\ &= \sum_{kl} a_{kl}\,\mathrm{Tr}(E_{ij}E_{kl}) \\ &= a_{ji} \end{aligned}$$

d'où l'unicité de $A$.

**Synthèse** : posons $A = (f(E_{ji}))_{ij} \in \mathrm{M}_n(\mathbb{K})$. Pour tout $M = (m_{ij})_{ij} \in \mathrm{M}_n(\mathbb{K})$, on a

$$\begin{aligned} \mathrm{Tr}(AM) &= \sum_{i=1}^{n} (AM)_{ii} \\ &= \sum_{i,j=1}^{n} f(E_{ji}) mji \\ &= f\left(\sum_{i,j=1}^{n} m_{ji}E_{ji}\right) \\ &= f(M) \end{aligned}$$

d'où l'existence de $A$.

**On munit $\mathrm{M}_n(\mathbb{R})$ de la norme subordonnée à la norme euclidienne sur $\mathbb{R}^n$. Notons $B$ la boule unité fermée de $\mathrm{M}_n(\mathbb{R})$ et $K$ l'enveloppe convexe de $\mathrm{O}_n(\mathbb{R})$. Montrons que $B = K$.**

Pour tout $M \in \mathrm{O}_n(\mathbb{R})$, on a

$$\|M\| = \sup_{\substack{x \in \mathbb{R}^n \\ x \neq 0}} \frac{\|Mx\|}{\|x\|} = \sup_{\substack{x \in \mathbb{R}^n \\ x \neq 0}} \frac{\|x\|}{\|x\|} = 1.$$

Ainsi, $B$ est convexe et contient $\mathrm{O}_n(\mathbb{R})$ donc elle contient $K$.
Raisonnons par l'absurde et supposons qu'il existe $M \in B \backslash K$. D'après le théorème de Carathéodory, l'application

$$\begin{aligned} \mathrm{O}_n(\mathbb{R})^{n^2+1} \times \Delta &\to K \\ (A_1, \ldots, A_{n^2+1}, t_1, \ldots, t_{n^2+1}) &\mapsto \sum_{i=1}^{n^2+1} t_i A_i \end{aligned}$$

où $\Delta = \{(t_1, \dots, t_{n^2+1} \in \mathbb{R}_+^{n^2+1} \mid t_1 + \cdots + t_{n^2+1} = 1\}$ est surjective donc $K$ est l'image continue d'un compact : c'est un compact. En particulier, on peut séparer strictement $\{M\}$ et $K$ par un hyperplan affine $H$. D'après le lemme précédent, il existe donc $A \in \mathrm{M}_n(\mathbb{R})$ non nulle et $s \in \mathbb{R}$ tels que pour tout $B \in K$, $\mathrm{Tr}(AB) < s < \mathrm{Tr}(AM)$. En particulier, on a

$$\sup_{B \in K} \mathrm{Tr}(AB) < \mathrm{Tr}(AM).$$

Posons $A = OS$ la décomposition polaire de $A$ et fixons $e_1, \dots, e_n \in \mathbb{R}^n$ une base orthonormée qui diagonalise $S$. On a

$$\begin{aligned}
\mathrm{Tr}(AM) &= \mathrm{Tr}(MA) \\
&= \sum_{i=1}^{n} \langle MAe_i, e_i \rangle \\
&= \sum_{i=1}^{n} \langle Ae_i, M^* e_i \rangle \\
&\leqslant \sum_{i=1}^{n} \|Ae_i\| \|M^* e_i\| \\
&= \sum_{i=1}^{n} \|OSe_i\| \\
&= \sum_{i=1}^{n} \|Se_i\| \\
&= \sum_{i=1}^{n} \langle Se_i, e_i \rangle \\
&= \sum_{i=1}^{n} \langle O^{-1}Ae_i, e_i \rangle \\
&= \mathrm{Tr}\big(AO^{-1}\big)
\end{aligned}$$

ce qui est absurde puisque $O^{-1} \in \mathrm{O}_n(\mathbb{R}) \subset K$. Ainsi, $M$ n'existe pas et $K = B$.

# Précisions :

**Séparation de $\{M\}$ et K par un hyperplan affine** :

# Réduction de Jordan par la dualité

## Cadre :

Soit $E$ un espace vectoriel de dimension finie. Tout endomorphisme de $E$ dont le polynôme caractéristique est scindé admet une forme réduite de Jordan.

**Recasages** :

- 150 Polynômes d'endomorphismes, réduction
- 156 Endomorphismes trigonalisables et nilpotents
- 159 Formes linéaires et dualité
- 162 Systèmes linéaires

**Référence** : Mathématiques pour l'agrégation, Rombaldi.

## Développement :

**Soit $u \in L(E)$ nilpotent d'indice $q$. Soit $x \in E$ vérifiant $u^{q-1}(x) \neq 0$. Montrer que $(x, u(x), \dots, u^{q-1}(x))$ est libre et engendre un sous-espace stable par $u$.**

Soient $\lambda_0, \dots, \lambda_{q-1} \in \mathbb{K}$ tels que $\sum_i \lambda_i u^i(x) = 0$. En appliquant $u^{q-1}$, on obtient $\lambda_0 u^{q-1}(x) = 0$ et donc $\lambda_0 = 0$ puisque $u^{q-1}(x) \neq 0$. Supposons que l'on sache que $\lambda_0 = \dots = \lambda_i = 0$. Alors, en appliquant $u^{q-i-2}$ à l'égalité, on obtient $\lambda_{i+1} u^{q-1}(x) = 0$ et donc $\lambda_{i+1} = 0$ puisque $u^{q-1}(x) \neq 0$.
Ainsi, par récurrence, on a $\lambda_0 = \dots = \lambda_{q-1} = 0$ et la famille est libre.
De plus, $\mathrm{Vect}(x, u(x), \dots, u^{q-1}(x)) = \mathbb{K}[u](x)$ donc c'est bien un sous-espace vectoriel stable par $u$.

**Soit $u \in L(E)$ nilpotent d'indice $q$. Construisons $\varphi \in E^*$ et $x \in E$ tels que $\mathrm{Vect}(x, u(x), \dots, u^{q-1}(x))$ et $\mathrm{Vect}(\varphi, u^T(\varphi), \dots, (u^T)^{q-1}(\varphi))^\circ$ soient supplémentaires dans $E$ et stables par $u$.**

$u$ étant nilpotent d'indice $q$, $u^T$ l'est aussi. Il existe donc $\varphi \in E^*$ tel que $\varphi \circ u^{q-1} \neq 0$ et il existe également $x \in E$ tel que $\varphi \circ u^{q-1}(x) \neq 0$. En particulier, on a $u^{q-1}(x) \neq 0$ et le lemme précédent nous assure que si

$$F = \mathrm{Vect}(x, u(x), \dots, u^{q-1}(x)) \quad \text{et} \quad G = \mathrm{Vect}(\varphi, \varphi \circ u, \dots, \varphi \circ u^{q-1}),$$

$F$ et $G^\circ$ sont stables par $u$ et de plus, on a

$$\dim F + \dim G^\circ = q + n - q = n$$

donc il nous suffit de montrer que $F \cap G^\circ = \{0\}$.
Fixons donc $y = \sum_i \lambda_i u^i(x) \in F \cap G^\circ$. En appliquant $\varphi \circ u^{q-1}$, on obtient $\lambda_0 \varphi \circ u^{q-1}(x) = 0$ et donc $\lambda_0 = 0$ puisque $\varphi \circ u^{q-1}(x) \neq 0$. Supposons que l'on sache que $\lambda_0, \dots, \lambda_i = 0$. En appliquant $\varphi \circ u^{q-i+2}$, on obtient $\lambda_{i+1} \varphi \circ u^{q-1}(x) = 0$ et donc $\lambda_{i+1} = 0$ puisque $\varphi \circ u^{q-1}(x) \neq 0$. Ainsi, par récurrence, on a $\lambda_0 = \dots = \lambda_{q-1} = 0$ et $y = 0$.
Finalement, $F \cap G = \{0\}$ et $F \oplus G = E$.

**Soit $u$ un endomorphisme de $E$. Montrons que $u$ admet une réduite de Jordan.**

On traite tout d'abord le cas où $u$ est nilpotent par récurrence forte sur $n = \dim(E)$.

**Initialisation** : si $n = 1$, $u = 0$ et il n'y a rien à montrer.

**Hérédité** : soit $n \in \mathbb{N}$ tel que la propriété soit vraie aux rangs $1, \dots, n$. Soit $E$ un espace vectoriel de dimension $n+1$ et soit $u \in L(E)$ un ensemble nilpotent d'indice $q$. Si $q = n+1$, le premier lemme donne une base dans laquelle $u$ est une matrice de Jordan. On suppose donc que $1 \leqslant q \leqslant n$. Considérons les sous-espaces $F$ et $G^\circ$ du deuxième lemme. La matrice de $u_{|F}$ dans la base $(x, u(x), \dots, u^{q-1}(x))$ est $J_q$ donc en complétant cette famille en une base de $E$ via une base de $G^\circ$, $u$ s'écrit matriciellement sous la forme

$$\begin{pmatrix} J_q & 0 \\ 0 & B \end{pmatrix}$$

où $B \in M_{n+1-q}(\mathbb{K})$ est nilpotente. L'hypothèse de récurrence permet alors de conclure.

**Conclusion** : par le principe de récurrence, la propriété est vraie pour tout $n \geqslant 1$.
Considérons le cas général. D'après le lemme des noyaux appliqué à $\chi_u = \prod_k (X - \lambda_k)^{\alpha_k}$, on a

$$E = \bigoplus_k \ker(u - \lambda_k \mathrm{id})^{\alpha_k}.$$

Ainsi, on peut appliquer ce qui précède aux endomorphismes $(u - \lambda_k \mathrm{id})_{|\ker(u-\lambda_k \mathrm{id})^{\alpha_k}}$ et concaténer les bases obtenues pour obtenir la forme réduite de Jordan voulue.

# Formule de Stirling via le TCL

## Cadre :

On a l'équivalent $n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)$.

**Recasages** :

- 223 Suites numériques
- 224 Développements asymptotiques
- 235 Interversion de symboles en analyse
- 236 Méthodes de calcul d'intégrales
- 261 Loi d'une variable aléatoire
- 262 Convergence d'une suite de variables aléatoires
- 264 Variables aléatoires discrètes
- 266 Utilisation de l'indépendance en probabilités

**Référence** : 131 développements pour l'oral.

## Développement :

**On se donne une suite $(X_n)_{n\in\mathbb{N}}$ de variables aléatoires i.i.d. suivant une loi de Poisson de paramètre 1 et on pose $Z_n = \frac{X_1+\cdots+X_n-n}{\sqrt{n}}$.**
**Nous allons montrer que**

$$\lim_{n\to+\infty}\int_0^{+\infty}\mathbb{P}(Z_n>t)\mathrm{d}t = \int_0^{+\infty}\mathbb{P}(Z>t)$$

**puis calculer les deux membres de cette égalité.**

• Remarquons tout d'abord que les fonctions $t\mapsto\mathbb{P}(Z_n>t)$ et $t\mapsto\mathbb{P}(Z>t)$ sont décroissantes donc mesurables. D'après le TCL, si $Z$ est une variable aléatoire de loi $\mathcal{N}(0,1)$, on a $Z_n \xrightarrow[n\to+\infty]{\text{Loi}} Z$. La loi de $Z$ étant sans atome, le théorème porte-manteau donne

$$\forall t>0,\quad \mathbb{P}(Z_n>t)\xrightarrow[n\to+\infty]{}\mathbb{P}(Z>t).$$

De plus, $\mathbb{E}(Z_n)=0$ et $\mathbb{V}(Z_n)=1$ donc $\mathbb{E}(Z_n^2)=1$ et l'inégalité de Markov donne

$$\forall t>1,\quad \mathbb{P}(Z_n>t)\leqslant\mathbb{P}(Z_n^2\geqslant t^2)\leqslant\frac{\mathbb{E}(Z_n^2)}{t^2}=\frac{1}{t^2}$$

donc on a

$$\forall t>0,\quad \mathbb{P}(Z_n>t)\leqslant\mathbb{1}_{]0,1]}(t)+\frac{1}{t^2}\mathbb{1}]1,+\infty[$$

et ce majorant est intégrable sur $\mathbb{R}_+$. Ainsi, le théorème de convergence dominée s'applique donne l'égalité voulue.

• Fixons $n\in\mathbb{N}^*$. La variable $X_1+\cdots+X_n$ suivant une loi de Poisson de paramètre $n$, on a

$$\begin{aligned}
\int_0^{+\infty}\mathbb{P}(Z_n>t)\mathrm{d}t &= \int_0^{+\infty}\mathbb{P}(X_1+\cdots+X_n>\sqrt{n}t+n)\mathrm{d}t\\
&= \int_0^{+\infty}\sum_{k=0}^{+\infty}e^{-n}\mathbb{1}_{k>\sqrt{n}t+n}\frac{n^k}{k!}\mathrm{d}t\\
&= \sum_{k=n+1}^{+\infty}e^{-n}\frac{n^k}{k!}\int_0^{\frac{k-n}{\sqrt{n}}}\mathrm{d}t\\
&= \sum_{k=n+1}^{+\infty}e^{-n}\frac{n^k}{k!}\frac{k-n}{\sqrt{n}}\\
&= \frac{e^{-n}}{\sqrt{n}}\sum_{k=n+1}^{+\infty}\frac{n^k}{k!}(k-n)
\end{aligned}$$

$$
\begin{aligned}
&= \frac{e^{-n}}{\sqrt{n}} \sum_{k=n+1}^{+\infty} \frac{n^k}{(k-1)!} - \frac{e^{-n}}{\sqrt{n}} \sum_{k=n+1}^{+\infty} \frac{n^{k+1}}{k!} \\
&= \frac{e^{-n}}{\sqrt{n}} \sum_{k=n}^{+\infty} \frac{n^{k+1}}{k!} - \frac{e^{-n}}{\sqrt{n}} \sum_{k=n+1}^{+\infty} \frac{n^{k+1}}{k!} \\
&= \frac{e^{-n}}{\sqrt{n}} \frac{n^{n+1}}{n!} \\
&= \sqrt{n} \left(\frac{n}{e}\right)^n \frac{1}{n!}.
\end{aligned}
$$

- On a

$$
\begin{aligned}
\int_0^{+\infty} \mathbb{P}(Z > t) \mathrm{d}t &= \int_0^{+\infty} \int_t^{+\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{u^2}{2}} \mathrm{d}u \, \mathrm{d}t \\
&= \int_0^{+\infty} \int_0^{+\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{u^2}{2}} \mathbb{1}_{t<u} \mathrm{d}u \, \mathrm{d}t \\
&= \int_0^{+\infty} \int_0^{+\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{u^2}{2}} \mathbb{1}_{t<u} \mathrm{d}t \, \mathrm{d}u \\
&= \int_0^{+\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{u^2}{2}} \int_0^u \mathrm{d}t \, \mathrm{d}u \\
&= \int_0^{+\infty} \frac{1}{\sqrt{2\pi}} u e^{-\frac{u^2}{2}} \, \mathrm{d}u \\
&= \frac{1}{\sqrt{2\pi}} [-e^{-\frac{u^2}{2}}]_{u=0}^{u \to +\infty} \\
&= \frac{1}{\sqrt{2\pi}}.
\end{aligned}
$$

Ainsi,

$$
\sqrt{n} \left(\frac{n}{e}\right)^n \frac{1}{n!} \xrightarrow[n \to +\infty]{} \frac{1}{\sqrt{2\pi}},
$$

ce qui se réécrit sous la forme

$$
\sqrt{2\pi n} \left(\frac{n}{e}\right)^n \frac{1}{n!} \xrightarrow[n \to +\infty]{} 1,
$$

c'est-à-dire

$$
n! \underset{+\infty}{\sim} \sqrt{2\pi n} \left(\frac{n}{e}\right)^n.
$$

# Développement eulérien de zêta

## Cadre :

Soit $(p_n)_{n\in\mathbb{N}}$ la suite des nombres premiers. Pour tout $s > 1$, on a $\frac{1}{\zeta(s)} = \prod_{n\in\mathbb{N}}(1 - p_n^{-s})$. On en déduit que la série $\sum_{n\in\mathbb{N}} \frac{1}{p_n}$ diverge.

**Recasages** :

- 264 Variables aléatoires discrètes
- 266 Utilisation de l'indépendance en probabilités

**Référence** : De l'intégration aux probabilités - Garet et Kurtzmann.

## Développement :

**Montrons que** $\frac{1}{\zeta(s)} = \prod_{n\in\mathbb{N}}(1 - p_n^{-s})$

Fixons $s > 1$. On considère la mesure $\mu_s$ sur $(\mathbb{N}^*, \mathcal{P}(\mathbb{N}^*))$ définie par

$$\mu_s(\{n\}) = \frac{1}{\zeta(s)}\frac{1}{n^s}.$$

Si $n \in \mathbb{N}^*$, on a

$$\mu_s(n\mathbb{N}^*) = \frac{1}{\zeta(s)}\sum_{k\geqslant 1}\frac{1}{n^s k^s} = \frac{1}{n^s}.$$

Posons $(p_k)_{k\geqslant 1}$ la suite des nombres premiers de $(A_k)_{k\geqslant 1} = (p_k\mathbb{N}^*)_{k\geqslant 1}$.
On a

$$\bigcap_{k\geqslant 1} A_k^c = \{n \in \mathbb{N}^* \mid n \text{ n'est divisible par aucun nombre premier } \} = \{1\}$$

donc en posant $B_k = \bigcap_{j=1}^{k} A_j^c$, on a

$$\begin{aligned}
\frac{1}{\zeta(s)} &= \mu_s(\{1\}) \\
&= \mu_s\left(\bigcap_{k\geqslant 1} A_k^c\right) \\
&= \mu_s\left(\bigcap_{k\geqslant 1} B_k^c\right) \\
&= \lim_{N\to+\infty} \mu_s\left(\bigcap_{k=1}^{N} B_k^c\right) \\
&= \lim_{N\to+\infty} \mu_s\left(\bigcap_{k=1}^{N} A_k^c\right).
\end{aligned}$$

Montrons finalement que les $(A_k)_{k\geqslant 1}$ sont indépendants. Soit $J \subset\subset \mathbb{N}^*$. On a

$$\begin{aligned}
\mu_s\left(\bigcap_{j\in J} A_j\right) &= \mu_s\left(\bigcap_{j\in J} p_j\mathbb{N}^*\right) \\
&= \mu_s\left(\text{PPCM}(p_j,\, j \in J)\mathbb{N}^*\right) \\
&= \mu_s\left(\prod_{j\in J} p_j\mathbb{N}^*\right)
\end{aligned}$$

$$= \frac{1}{\prod_{j\in J} p_j^s}$$
$$= \prod_{j\in J} \frac{1}{p_j^s}$$
$$= \prod_{j\in J} \mu_s(A_j)$$

donc ces évènements sont indépendants et leurs complémentaires aussi. Finalement, on a

$$\begin{aligned}\frac{1}{\zeta(s)} &= \lim_{N\to+\infty} \mu_s\left(\bigcap_{k=1}^{N} A_k^c\right)\\ &= \lim_{N\to+\infty} \prod_{k=1}^{N} \mu_s(A_k^c)\\ &= \lim_{N\to+\infty} \prod_{k=1}^{N} (1-\mu_s(A_k))\\ &= \lim_{N\to+\infty} \prod_{k=1}^{N} \left(1-\frac{1}{p_k^s}\right)\\ &= \prod_{k=1}^{\infty} \left(1-\frac{1}{p_k^s}\right)\end{aligned}$$

d'où

$$\zeta(s) = \prod_{k=1}^{\infty} \left(1-\frac{1}{p_k^s}\right)^{-1}.$$

**Montrons que $\zeta(s) \xrightarrow[s\to 1^+]{} +\infty$.**

Une comparaison série-intégrale donne, pour tout $s > 1$ :

$$1 + \int_2^{+\infty} \frac{1}{t^s}\mathrm{d}t \leqslant \sum_{n=1}^{\infty} \frac{1}{n^s} \leqslant 1 + \int_1^{+\infty} \frac{1}{t^s}\mathrm{d}t$$

d'où

$$1 + \frac{1}{s-1}\frac{1}{2^{s-1}} \leqslant \zeta(s) \leqslant 1 + \frac{1}{s-1},$$

c'est-à-dire

$$s - 1 + \frac{1}{2^{s-1}} \leqslant (s-1)\zeta(s) \leqslant s.$$

En faisant tendre $s$ vers $1^+$, on trouve donc $\zeta(s) \underset{s\to 1^+}{\sim} \frac{1}{s-1}$ et donc $\zeta(s) \xrightarrow[s\to 1^+]{} +\infty$.

**Montrons que $\displaystyle\sum_{n\in\mathbb{N}} \frac{1}{p_n} = +\infty$**

Raisonnons par l'absurde et supposons que $\sum_n \frac{1}{p_n}$ converge. Alors, par équivalence, la série $\sum_n -\ln\left(1-\frac{1}{p_n}\right)$ converge également. Or, par comparaison, on a

$$-\ln\left(1-\frac{1}{p_n^s}\right) \leqslant -\ln\left(1-\frac{1}{p_n}\right)$$

pour tout $s > 1$ donc on obtient, en appliquant l'exponentielle :

$$\ln\left(\prod_n \left(1-\frac{1}{p_n^s}\right)^{-1}\right) \leqslant \ln\left(\prod_n \left(1-\frac{1}{p_n}\right)^{-1}\right)$$

pour tout $s > 1$, c'est-à-dire

$$\ln(\zeta(s)) \leqslant \ln\left(\prod_n \left(1-\frac{1}{p_n}\right)^{-1}\right)$$

pour tout $s > 1$. Ceci entre en contradiction avec le fait que $\ln(\zeta(s)) \xrightarrow[s\to 1^+]{} +\infty$ donc on peut conclure que

$$\sum_n \frac{1}{p_n} = +\infty.$$

# Groupe simple d'ordre 60

## Cadre :

$\mathfrak{A}_5$ est le seul groupe simple d'ordre 60.

**Recasages** :

- 101 Groupes opérant sur un ensemble
- 103 Conjugaison dans un groupe, quotients
- 104 Groupes finis
- 105 Groupe symétrique

**Référence** :

## Développement :

**Soit $G$ un groupe simple d'ordre 60. Montrons que $G \simeq \mathfrak{A}_5$.**

On va montrer que $G$ agit non trivialement sur un ensemble à 5 éléments. Nous allons raisonner par l'absurde en supposant l'hypothèse

$$(H) : G \text{ n'admet pas de sous-groupe strict d'indice } \leqslant 5.$$

Pour $p \in \mathbb{P}$, notons $E_p(G)$ l'ensemble des $p$-Sylow de $G$ et $n_p$ le cardinal de $E_p(G)$. L'action de $G$ sur ses 2-Sylow étant transitive, $n_2$ est l'indice d'un stabilisateur, donc d'un sous-groupe de $G$. Comme $|G| = 60 = 2^2 \cdot 3 \cdot 5$, on a $n_2 \mid 15$ donc $n_2 \in \{1, 3, 5, 15\}$ mais par $(H)$, on ne peut avoir que $n_2 \in \{1, 15\}$. $G$ étant simple, on ne peut pas avoir $n_2 = 1$ d'où $n_2 = 15$.
Comptons maintenant le nombre d'éléments présents dans ces 2-Sylow. Soient $S_1$ et $S_2$ deux 2-Sylow distincts de $G$. Si $g \in S_1 \cap S_2$. Considérons le centralisateur $N_G(g)$ de $g$ dans $G$. On a

$$\begin{cases} o(N_G(g)) > 4 \text{ car } N_G(g) \supset S_1 \cup S_2, \\ 4 \mid o(N_G(g)) \text{ car } N_G(g) \subset S_1, \\ o(N_G(g)) \mid 60 \text{ car } N_G(g) \subset G. \end{cases}$$

Ainsi, on a $o(N_G(g)) \in \{12, 20, 60\}$ mais $(H)$ implique que $o(N_G(g)) \neq 12, 20$ donc $o(N_G(g)) = 60$ et $g \in Z(G) = \{e_G\}$ (car $G$ simple d'ordre non premier). Ainsi, on a $S_1 \cap S_2 = \{e_G\}$.
$G$ contient donc $3 \cdot 15 = 45$ éléments d'ordre 2 ou 4.
Comptons maintenant les éléments d'ordre 5 de $G$. On a $n_5 \mid 12$ et $n_5 \equiv 1 \pmod 5$ donc $n_5 \in \{1, 6\}$ et une fois de plus, $G$ est simple donc $n_5 \neq 1$ ce qui implique que $n_5 = 6$. Les 5-Sylow de $G$ étant de cardinal premier 5, deux 5-Sylow distincts s'intersectent trivialement et $G$ possède $4 \cdot 6 = 24$ éléments d'ordre 5.
On a donc montré que $G$ possède au moins $45 + 24 = 69$ éléments, ce qui est absurde puisque $|G| = 60$. On en conclut que l'hypothèse $(H)$ est erronée.
Soit $K \subset G$ un sous-groupe strict d'indice inférieur ou égal à 5.
Si $|G : H| = 5$, l'action (transitive donc non-triviale) de $G$ sur $G/H$ fournit un morphisme $G \to \mathfrak{S}_5$. Ce morphisme étant non-trivial et $G$ étant simple, il est injectif et $G$ s'identifie à sous-groupe d'indice 2 de $S_5$. Par unicité, de ce dernier, on obtient un isomorphisme entre $G$ et $\mathfrak{A}_5$.
Si $|G : H| \leqslant 4$, le même raisonnement implique que $G$ est isomorphe à un sous-groupe de $\mathfrak{S}_{|G:H|}$, ce qui est absurde puisque

$$|G| = 60 > |G : H|! = |\mathfrak{S}_{|G:H|}|.$$

**Montrons que $\mathfrak{A}_5$ est simple.**

Le groupe $\mathfrak{A}_5$ contient :

- 1 neutre,
- 20 3-cycles,
- 24 5-cycles,
- 15 bitranspositions.

Soit $H \triangleleft \mathfrak{A}_5$ différent de $\{\mathrm{id}\}$. Si $H$ contient un 3-cycle, il les contient tous et comme ils engendrent $\mathfrak{A}_5$, on a $H = \mathfrak{A}_5$.
Supposons que $H$ ne contienne pas de 3-cycle. Supposons de plus que $H$ contienne un 5-cycle. Les 5-Sylow de $\mathfrak{A}_5$ étant de cardinal 5, ils sont engendrés par les 5-cycles. Or, $\mathfrak{A}_5$ agit transitivement sur ses 5-Sylow donc $H$ contient tous les 5-Sylow de $\mathfrak{A}_5$ et donc tous les 5-cycles de $\mathfrak{A}_5$. Puisque $25 \not| \, |\mathfrak{A}_5|$, $H$ contient également une bitransposition $(ij)(kl)$. On a alors

$$(ij)(kl)(klijm) = (mlj) \in H,$$

ce qui est absurde.
Ainsi, $H$ ne peut pas contenir de 5-cycle et il ne contient que des bitranspositions. Pour tout $g \in H$, on a donc $g^2 = \mathrm{id}$ et donc $H$ est un 2-groupe. Il est même de cardinal 2 ou 4 d'après le théorème de Lagrange. Si $H$ était de cardinal 2, il contiendrait un élément non nul et central dans $\mathfrak{A}_5$ ce qui est absurde donc $H$ est de cardinal 4. $H$ est donc un 2-Sylow distingué de $\mathfrak{A}_5$ mais ce dernier admet plusieurs 2-Sylow : $\{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ et $\{\mathrm{id}, (23)(45), (24)(35), (25)(35)\}$ par exemple, donc $H$ ne peut pas être distingué, ce qui est absurde.
Ainsi, le seul cas possible est le cas $H = \mathfrak{A}_5$ et donc $\mathfrak{A}_5$ est simple.

# Théorème de Weierstrass via la convolution

## Cadre :

Soit $(u_i)_{i\in I}$ une famille de fonctions vérifiant :

1. $u_i \geqslant 0$,
2. $\int_{\mathbb{R}} u_i(y)\mathrm{d}y = 1$,
3. $\forall \delta > 0$, $\int_{|y|>\delta} u_i(y)\mathrm{d}y \xrightarrow[i\to+\infty]{} 0$.

Alors, pour toute fonction $f$ continue à support compact, on a $f * u_i \to f$ uniformément. On en déduit que l'ensemble des fonctions polynomiales (resp. trigonométriques) est uniformément dense dans $C([a,b])$.

**Recasages** :

- 201 Espaces de fonctions
- 209 Approximation par des fonctions régulières
- 228 Continuité et dérivabilité de la variable réelle
- 234 Fonctions Lebesgue-intégrables
- 241 Suites et séries de fonctions

**Référence** :

## Développement :

Fixons $f$ continue à support compact et $\varepsilon > 0$. Par le théorème de Heine, $f$ est uniformément continue donc il existe $\delta > 0$ tel que

$$|x-y| \leqslant \delta \implies |f(x)-f(y)| \leqslant \varepsilon.$$

Pour tout $x \in \mathbb{R}$, on a alors

$$\begin{aligned}
|f*u_i(x) - f(x)| &= \left|\int_{\mathbb{R}} f(x-y)u_i(y)\mathrm{d}y - f(x)\right| \\
&= \left|\int_{\mathbb{R}} u_i(y)(f(x-y)-f(x))\mathrm{d}y\right| \\
&\leqslant \int_{\mathbb{R}} u_i(y)|f(x-y)-f(x)|\mathrm{d}y \\
&= \int_{|y|>\delta} u_i(y)|(f(x-y)-f(x))|\mathrm{d}y + \int_{|y|<\delta} u_i(y)|(f(x-y)-f(x))|\mathrm{d}y \\
&\leqslant 2\|f\|_\infty \int_{|y|>\delta} u_i(y)\mathrm{d}y + \varepsilon \int_{|y|<\delta} u_i(y)\mathrm{d}y \\
&\leqslant 2\|f\|_\infty \int_{|y|>\delta} u_i(y)\mathrm{d}y + \varepsilon.
\end{aligned}$$

Cette majoration étant indépendante de $x$, on a

$$\|f*u_i - f\|_\infty \leqslant 2\|f\|_\infty \int_{|y|>\delta} u_i(y)\mathrm{d}y + \varepsilon.$$

De plus, on a par hypothèse

$$\int_{|y|>\delta} u_i(y)\mathrm{d}y \xrightarrow[i\to+\infty]{} 0$$

donc en fixant $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N, \quad \left|\int_{|y|>\delta} u_n(y)\mathrm{d}y\right| \leqslant \frac{\varepsilon}{\|f\|_\infty},$$

on a

$$\forall n \geqslant N, \quad \|f*u_i - f\|_\infty \leqslant 2\varepsilon.$$

Considérer maintenant la suite de fonctions définies sur $\mathbb{R}$ par

$$u_n(t) = \begin{cases} \frac{1}{a_n}(1-t^2)^n \text{ si } t \in [-1,1] \\ 0 \text{ sinon} \end{cases}$$

où

$$a_n = \int_{-1}^{1} (1-t^2)^n \mathrm{d}t.$$

Les conditions 1. et 2. sont alors vérifiées. De plus, si $\delta > 0$, on a

$$2\int_{\delta}^{1} (1-t^2)^n \mathrm{d}t \geqslant 2(1-\delta)(1-\delta^2)^n$$

et

$$a_n = 2\int_0^1 (1-t^2)^n \mathrm{d}t \geqslant 2\int_0^1 (1-t)^n \mathrm{d}t = \frac{-2}{n+1}\Big[(1-t)^{n+1}\Big]_0^1 = \frac{2}{n+1}$$

d'où

$$\int_{|t|>\delta} u_n(t)\mathrm{d}t \leqslant (1-\delta)(n+1)(1-\delta^2)^n \xrightarrow[n\to+\infty]{} 0.$$

Ainsi, $(u_n)_n$ est une approximation de l'identité.
Supposons que $\mathrm{supp}(f) \subset [-\frac{1}{2}, \frac{1}{2}]$. Alors, pour tout $x \in [-\frac{1}{2}, \frac{1}{2}]$, on a

$$\begin{aligned} u_n * f(x) &= \int_{-\frac{1}{2}}^{\frac{1}{2}} u_n(x-y) f(y)\mathrm{d}y \\ &= \int_{-\frac{1}{2}}^{\frac{1}{2}} \frac{1}{a_n}(1-(x-y)^2)^n f(y)\mathrm{d}y. \end{aligned}$$

En développant le terme $(1-(x-y)^2)^n$ puis en utilisant la linéarité de l'intégrale, on montre que $u_n * f_{|[-\frac{1}{2},\frac{1}{2}]}$ est polynomiale. Comme elle converge uniformément vers $f$, on en déduit que $f$ est limite uniforme d'une suite de polynômes.
Si $f$ est supportée dans $[a,b]$, un changement de variable affine permet de se ramener au cas où $f$ est à support dans $[-\frac{1}{2}, \frac{1}{2}]$.
Enfin, si $f \in C([a,b])$, on peut prolonger $f$ en une fonction continue à support compact et appliquer ce qui précède.

# Théorèmes d'Abel et Taubérien faible

## Cadre :

Soit $\sum_n a_n z^n$ une série entière de rayon de convergence $\geqslant 1$ telle que $\sum_n a_n$ converge. La série de fonctions $\sum_{n=0}^{+\infty} a_n z^n$ converge uniformément sur $[0,1]$. En particulier, on a

$$\lim_{\substack{z\to 1\\ z\in[0,1]}} \sum_{n=0}^{+\infty} a_n z^n = \sum_{n=0}^{+\infty} a_n.$$

Réciproquement, si $\sum_n a_n z^n$ est une série entière de rayon de convergence 1 vérifiant $a_n = o\left(\frac{1}{n}\right)$, si $f$ la somme de cette série entière sur le $[0,1[$ et si la limite $\ell = \lim_{\substack{x\to 1\\ x<1}} f(x)$ existe alors

$$\sum_{n=0}^{+\infty} a_n = \ell.$$

**Recasages** :

- 230 Séries numériques, restes et sommes partielles
- 235 Interversion de symboles en analyse
- 241 Suites et séries de fonctions
- 243 Séries entières, propriétés de la somme

**Référence** : Oraux X-ENS, Analyse 2

## Développement :

**Soit $(a_n)_n$ une suite de nombres complexes telle que le rayon de convergence de la série entière $\sum_n a_n z^n$ soit supérieur ou égal à 1. On suppose de plus que $\sum_n a_n$ converge. Montrons que $\sum_n a_n z^n$ converge uniformément sur $[0,1]$.**

Pour tout $n \geqslant 0$, on pose $r_n = \sum_{k=n+1}^{+\infty} a_k$. Soit $x \in [0,1[$. Pour tout $n \geqslant 1$, on a

$$\begin{aligned}
\sum_{k=n+1}^{+\infty} a_k x^k &= \sum_{k=n+1}^{+\infty} (r_{k-1} - r_k) x^k \\
&= \sum_{k=n+1}^{+\infty} r_{k-1} x^k - \sum_{k=n+1}^{+\infty} r_k x^k \\
&= \sum_{k=n}^{+\infty} r_k x^{k+1} - \sum_{k=n+1}^{+\infty} r_k x^k \\
&= r_n x^{n+1} + \sum_{k=n+1}^{+\infty} r_k (x^{k+1} - x^k) \\
&= r_n x^{n+1} + (x-1) \sum_{k=n+1}^{+\infty} r_k x^k
\end{aligned}$$

Soit maintenant $\varepsilon > 0$. La suite $(r_n)_n$ converge vers 0 donc il existe $N \in \mathbb{N}$ tel que pour tout $n \geqslant N$, $|r_n| \leqslant \varepsilon$. Alors, pour tout $n \geqslant N$ et tout $x \in [0,1[$, on a

$$\begin{aligned}
\left| \sum_{k=n+1}^{+\infty} a_k x^k \right| &= \left| r_n x^{n+1} + (x-1) \sum_{k=n+1}^{+\infty} r_k x^k \right| \\
&\leqslant |r_n x^{n+1}| + |x-1| \sum_{k=n+1}^{+\infty} |r_k x^k|
\end{aligned}$$

$$\begin{aligned}
&\leqslant \varepsilon + (1-x)\sum_{k=n+1}^{+\infty} \varepsilon x^k \\
&= \varepsilon + \varepsilon x^{n+1} \\
&\leqslant 2\varepsilon.
\end{aligned}$$

De plus, $\left|\sum_{k=n+1}^{+\infty} a_k 1^k\right| = |r_n| \leqslant \varepsilon \leqslant 2\varepsilon$ donc $\sup_{x\in[0,1]} \left|\sum_{k=n+1}^{+\infty} a_k x^k\right| \leqslant 2\varepsilon$, ce qui prouve la convergence uniforme sur $[0,1]$.

**Réciproquement, soit $(a_n)_{n\in\mathbb{N}}$ vérifiant $a_n = o\left(\frac{1}{n}\right)$ et dont le rayon de convergence de la série entière $\sum_n a_n z^n$ est 1. Notons $f$ sa somme. On suppose de plus que la limite $\ell = \lim_{x\to 1^-} f(x)$ existe.**

Pour $n \in \mathbb{N}^*$, on pose $S_n = \sum_{k=0}^n a_k$. Soit $x \in [0,1[$ et soit $n \in \mathbb{N}^*$. On a

$$|S_n - \ell| \leqslant |S_n - f(x)| + |f(x) - \ell|.$$

Il nous suffit donc de majorer la quantité $|S_n - f(x)|$. Remarquons que

$$\begin{aligned}
|S_n - f(x)| &= \left|\sum_{k=0}^n a_k(1-x^k) - \sum_{k=n+1}^{+\infty} a_k x^k\right| \\
&\leqslant \sum_{k=0}^n |a_k|(1-x^k) + \sum_{k=n+1}^{+\infty} |a_k| x^k \\
&\leqslant (1-x)\sum_{k=0}^n k|a_k| + \frac{1}{n}\sum_{k=n+1}^{+\infty} k|a_k|x^k.
\end{aligned}$$

Or, $ka_k \xrightarrow[k\to+\infty]{} 0$ donc $\sup_{k\geqslant n+1} k|a_k| \xrightarrow[n\to+\infty]{} 0$. On a alors

$$\begin{aligned}
|S_n - f(x)| &\leqslant (1-x)\sum_{k=0}^n k|a_k| + \sup_{k\geqslant n+1} k|a_k| \frac{1}{n}\sum_{k=n+1}^{+\infty} x^k \\
&\leqslant (1-x)\sum_{k=0}^n k|a_k| + \sup_{k\geqslant n+1} k|a_k| \frac{1}{n(1-x)} \\
&= (1-x)n\left(\frac{1}{n}\sum_{k=0}^n k|a_k|\right) + \sup_{k\geqslant n+1} k|a_k| \frac{1}{n(1-x)}.
\end{aligned}$$

De plus, le lemme de Cesàro nous assure que $\frac{1}{n}\sum_{k=0}^n k|a_k| \xrightarrow[n\to+\infty]{} 0$ donc il ne nous reste plus qu'à choisir le point $x \in [0,1[$ en lequel évaluer pour simplifier notre majoration. On choisit alors $x$ tel que $(1-x)n = 1$, c'est-à-dire $x = 1 - \frac{1}{n}$ et on obtient finalement

$$|S_n - \ell| \leqslant \frac{1}{n}\sum_{k=0}^n k|a_k| + \sup_{k\geqslant n+1} k|a_k| + \left|f\left(1-\frac{1}{n}\right) - \ell\right| \xrightarrow[n\to+\infty]{} 0.$$

Ainsi, $\sum_{k\geqslant 0} a_k$ converge et vaut $\ell$.

# Polynômes orthogonaux

## Cadre :

Considérons une fonction de poids $\rho$ sur un intervalle $I$ de $\mathbb{R}$. S'il existe $\alpha > 0$ tel que $\int_I e^{\alpha|x|}\rho(x)\mathrm{d}x$ alors il existe une unique famille totale orthogonale $(P_n)_{n\in\mathbb{N}}$ de $L^2(I,\rho)$ composée de polynômes unitaires échelonnés en degré.

**Recasages** :

- 234 Fonctions Lebesgue-intégrables
- 250 Transformation de Fourier
- 209 Approximation par des fonctions régulières
- 213 Espaces de Hilbert
- 245 Fonctions holomorphes et méromorphes
- 201 Espaces de fonctions
- 239 Intégrales à paramètres

**Référence** : Analyse de Fourier dans les espaces fonctionnels, El Amrani.

## Développement :

**Montrons que les polynômes sont bien dans $L^2(I,\rho)$**

Il suffit de remarquer que si $n \in \mathbb{N}$, on a $x^n = o(e^{\alpha|x|})$ en $+\infty$ et que $x^n$ est continue sur $I$.

**Construisons la suite $(P_n)_{n\in\mathbb{N}}$ via le procédé d'orthonormalisation de Gram-Schmidt.**

Le caractère unitaire et la contrainte en degré de ces polynômes forcent $P_0 = 1$. Supposons qu'on ait construit $P_0, \dots, P_n$. Comme $P_{n+1}$ doit être unitaire de degré $n+1$, on le cherche sous la forme $P_{n+1} = x^n - \sum_{k=0}^{n} a_k P_k$ où $a_0, \dots, a_n \in \mathbb{C}$. Les relations d'orthogonalités donnent alors

$$\forall j \in \{0,\dots,n\}, 0 = \langle P_{n+1}|P_j\rangle = \langle x^n|P_j\rangle - \sum_{k=0}^{n} a_k \langle P_k|P_j\rangle = \langle x^n|P_j\rangle - a_j \langle P_j|P_j\rangle$$

donc le polynôme

$$P_{n+1} = x^n - \sum_{k=0}^{n} \frac{\langle x^n|P_j\rangle}{\langle P_j|P_j\rangle} P_j$$

est l'unique polynôme cherché.

**Fixons $f \in L^2(I,\rho)$ telle que $\langle f|x^n\rangle = 0$ pour tout $n \in \mathbb{N}$. Montrons que $f = 0$.**

On pose $\varphi = f\rho\mathbb{1}_I$. Si $t \geqslant 0$, on a $t \leqslant \frac{1+t^2}{2}$ donc

$$\forall x \in I, \quad |f(x)|\rho(x) \leqslant \frac{1+|f(x)|^2}{2}\rho(x)$$

et $\rho, |f|^2\rho$ sont intégrables sur $I$ par hypothèse donc $\varphi$ est intégrable sur $\mathbb{R}$.

On considère la transformée de Fourier de $\varphi$ donnée par $\hat{\varphi}(\xi) = \int_{\mathbb{R}} \varphi(x)e^{-ix\xi}\mathrm{d}x$ que l'on prolonge à $B = \{z \in \mathbb{C} \mid |\operatorname{Im}(z)| < \frac{\alpha}{2}\}$. Montrons que $\hat{\varphi} : B \to \mathbb{C}$ est bien définie et holomorphe.
Si $z \in B$ et $x \in I$, on a $|f(x)e^{-izx}\rho(x)| = |f(x)|\rho(x)e^{\operatorname{Re}(-izx)} = |f(x)|\rho(x)e^{x\operatorname{Im}(z)} \leqslant |f(x)|\rho(x)e^{\frac{\alpha}{2}|x|}$. Or, par l'inégalité de Cauchy-Schwarz dans $L^2(I,\rho)$, on a

$$\int_I |f(x)|\rho(x)e^{\frac{\alpha}{2}|x|}\mathrm{d}x \leqslant \left(\int_I |f(x)|^2\rho(x)\mathrm{d}x\right)^{\frac{1}{2}} \left(\int_I e^{\alpha|x|}\rho(x)\mathrm{d}x\right)^{\frac{1}{2}} < +\infty$$

donc $\hat{\varphi}$ est bien définie. De plus, si $x \in \mathbb{R}$, l'application $z \mapsto f(x)e^{-izx}\rho(x)$ est holomorphe donc la majoration précédente implique par le théorème d'holomorphie des intégrales à paramètres que $\hat{\varphi}$ est holomorphe sur $B$. De plus, on a

$$\forall n \in \mathbb{N}, \forall z \in B, \quad \hat{\varphi}^{(n)}(z) = \int_I \frac{\partial^n}{\partial z^n} f(x)e^{-izx}\rho(x)\mathrm{d}x = (-i)^n \int_I x^n f(x)e^{-izx}\rho(x)\mathrm{d}x$$

et en particulier,

$$\forall n \in \mathbb{N}, \quad \hat{\varphi}^{(n)}(0) = (-i)^n \int_I x^n f(x)\rho(x)\mathrm{d}x = 0.$$

Comme $\hat{\varphi}$ est développable en série entière autour de 0 (car holomorphe), on en déduit que $\hat{\varphi} = 0$ sur un voisinage de 0, ce qui implique que $\hat{\varphi} = 0$ sur $B$ d'après le principe du prolongement analytique (car $B$ est connexe).
En particulier, $\hat{\varphi} = 0$ sur $\mathbb{R}$ et comme la transformation de Fourier est injective, cela donne $\varphi = 0$ sur $\mathbb{R}$, c'est-à-dire $f = 0$ $\lambda$-p.p. et donc $f = 0$ dans $L^2(I, \rho)$.
Finalement, $\mathrm{Vect}(x^n, n \in \mathbb{N})$ est dense dans $L^2(I, \rho)$.

# Isométries du cube et du tétraèdre

## Cadre :

Les groupes d'isométries du tétraèdre et du cube sont donnés par

$$\mathrm{Is}^+(\Delta_4) \simeq \mathfrak{A}_4, \quad \mathrm{Is}(\Delta_4) \simeq \mathfrak{S}_4, \quad \mathrm{Is}^+(C_6) \simeq \mathfrak{S}_4, \quad \mathrm{Is}(C_6) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}.$$

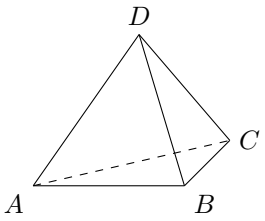
**Recasages** :

- 101 Groupes opérant sur un ensemble
- 104 Groupes finis
- 105 Groupe symétrique
- 108 Parties génératrices d'un groupe
- 161 Espaces vectoriels et affines euclidiens

**Référence** : NHGH2

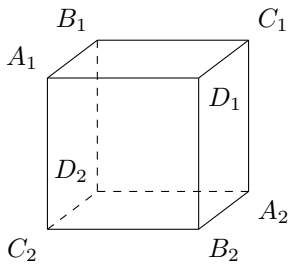
## Développement :

**Soit $\Delta_4$ un tétraèdre régulier dont les sommets sont $\mathcal{S} = \{A, B, C, D\}$. Montrons que $\mathrm{Is}(\Delta_4) \simeq \mathfrak{S}_4$.**




Considérons le morphisme $\varphi : \begin{array}{ccc} \mathrm{Is}(\Delta_4) & \to & \mathfrak{S}_4 \simeq \mathfrak{S}_{\mathcal{S}} \\ f & \mapsto & f_{|\mathcal{S}} \end{array}$. Il est injectif car $\mathcal{S}$ est un repère affine de l'espace. De plus, la symétrie orthogonale par rapport au plan passant par $C$, $D$ et $\mathrm{mil}(AB)$ échange $A$ et $B$ et fixe $C$ et $D$ donc toutes les transpositions sont dans $\mathrm{Im}(\varphi)$. Comme elles engendrent $\mathfrak{S}_4$, $\varphi$ est surjectif.
Ainsi, $\mathrm{Is}(\Delta_4) \simeq \mathfrak{S}_4$. Comme $\mathrm{Is}^-(\Delta_4) \neq \emptyset$, on a $|\mathrm{Is}(\Delta_4) : \mathrm{Is}^+(\Delta_4)| = 2$ et donc $\mathrm{Is}^+(\Delta_4) \simeq \mathfrak{A}_4$ car $\mathfrak{A}_4$ est l'unique sous-groupe d'indice 2 de $\mathfrak{S}_4$ (unicité de la signature car les transpositions engendrent $\mathfrak{S}_4$).

**Soit $C_6$ un cube dont les sommets sont $\mathcal{S} = \{A_1, B_1, C_1, D_1, A_2, B_2, C_2, D_2\}$. Montrons que $\mathrm{Is}^+(C_6) \simeq \mathfrak{S}_4$.**




Considérons les quatre grandes diagonales $\mathcal{D} = \{A, B, C, D\}$ de $C_6$. Ces diagonales ayant la plus grande distance possible dans le cube (par conservation de l'alignement des applications affines), toute isométrie laissant globalement stable le cube permute les éléments de $\mathcal{D}$.
On peut donc considérer le morphisme $\varphi : \begin{array}{ccc} \mathrm{Is}(C_6) & \to & \mathfrak{S}_4 \simeq \mathfrak{S}_{\mathcal{D}} \\ f & \mapsto & f_{|\mathcal{D}} \end{array}$. Montrons que $\varphi_{|\mathrm{Is}^+(C_6)}$ est injectif.
Soit $f \in \ker(\varphi)$. Comme $f$ laisse globalement invariante $\mathcal{D}$, $f(A_1) \in \{A_1, A_2\}$. Supposons que $f(A_1) = A_1$. Alors $f(B_1) = B_1$ car $A_1B_1 \neq A_1B_2$. De même, $f(D_1) = D_1$ donc $f$ fixe donc le repère affine $(A_1, B_1, D_1, B_2)$, d'où $f = \mathrm{id}$.
Considérons maintenant $f \in \ker(\varphi) \cap \mathrm{Is}^+(C_6)$. D'après la remarque précédente, si $f(A_1) = A_1$ alors $f = \mathrm{id}$. Au contraire, si $f(A_1) = A_2$ alors si $s$ désigne la symétrie centrale du cube, on a $f \circ s \in \ker(\varphi)$ et $f \circ s(A_1) = A_1$

d'où $f \circ s = \mathrm{id}$ d'après ce qui précède. Ainsi, on doit avoir $f = s$ ce qui est absurde puisque $f \in \mathrm{Is}^+(C_6)$. Finalement, $f = \mathrm{id}$ et $\varphi_{|\mathrm{Is}^+(C_6)}$ est injectif.
Enfin, si $r_H$ désigne le retournement orthogonal par rapport à l'hyperplan $H$ passant par $A_1, A_2, B_1, B_2$, on a $r_H \in \mathrm{Is}^+(C_6)$ et $\varphi(r_H)$ est la transposition échangeant $C$ et $D$ donc les transpositions sont dans $\mathrm{Im}(\varphi_{|\mathrm{Is}^+(C_6)})$. Comme elles engendrent $\mathfrak{S}_4$, $\varphi_{|\mathrm{Is}^+(C_6)}$ est surjectif et on a bien $\mathrm{Is}^+(C_6) \simeq \mathfrak{S}_4$.
Finalement, on a

— $\mathrm{Is}^+(C_6)\langle s\rangle = \mathrm{Is}(C_6)$,
— $\forall f \in \mathrm{Is}^+(C_6), g \in \langle s\rangle$, $g \circ s = s \circ g$,
— $\mathrm{Is}^+(C_6) \cap \langle s\rangle = \{\mathrm{id}\}$ car $\langle s\rangle = \{\mathrm{id}, s\}$,

donc $\mathrm{Is}(C_6) \simeq \mathrm{Is}^+(C_6) \times \langle s\rangle \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

# Théorème du point fixe de Kakutani

## Cadre :

Si $E$ est un espace euclidien, $G$ est un sous-groupe compact de $GL(E)$ et $K$ est un convexe non vide de $E$ stable par $G$, il existe un point fixe pour $G$ dans $K$.

Si $G$ est un sous-groupe compact de $GL(n,\mathbb{R})$ alors $G$ est conjugué à un sous-groupe de $O(n,\mathbb{R})$.

**Recasages** :

- 

**Référence** :

## Développement :

Quitte à remplacer $K$ par $\overline{\text{Conv}(G\cdot x)}$ pour un élément $x \in K$, on peut supposer $K$ compact. On définit $N : \begin{array}{ccc} E & \to & \mathbb{R}_+ \\ x & \mapsto & \sup\limits_{g\in G} \|g(x)\| \end{array}$. L'application $N$ est bien définie par compacité de $G$ et c'est clairement une norme sur $E$. Elle est de plus invariante par $G$ :

$$\forall g \in G, \forall x \in E,\ N(gx) = \sup_{h\in G} \|hg(x)\| = \sup_{h\in G} \|h(x)\| = N(x).$$

Par compacité de $K$, il existe $y \in G$ tel que $N(y) = \min\limits_{x\in G} N(x)$. Soit $g \in G$. On a

$$N(y) \leqslant N\left(\frac{y+g(y)}{2}\right) \leqslant \frac{1}{2}(N(y) + N(g(y))) = N(y)$$

donc $y$ et $g(y)$ vérifient un cas d'égalité dans l'inégalité triangulaire pour $N$. Étudions ce qu'elle implique. Comme $G$ est compact, il existe $h \in G$ tel que $N(y+g(y)) = \|h(y) + hg(y)\| \leqslant \|h(y)\| + \|hg(y)\| \leqslant N(y) + N(g(y))$. Le cas d'égalité implique que $\|h(y) + hg(y)\| = \|h(y)\| + \|hg(y)\|$ et donc qu'il existe $\lambda \in \mathbb{R}_+^*$ tel que $h(y) = \lambda hg(y)$ d'après le cas d'égalité pour une norme euclidienne. Comme $h$ est inversible, cela implique $y = \lambda g(y)$ et comme $N(y) = N(g(y))$, on a $\lambda = 1$ et $y = g(y)$. Ainsi, $y$ est le point fixe cherché.

Considérons l'action $\rho$ de $H$ sur $\mathcal{S}_n(\mathbb{R})$ donnée par

$$\forall A \in G, \forall B \in \mathcal{S}_n(\mathbb{R}),\ \rho(A)B = ABA^T.$$

L'action est continue car polynomiale et $\rho(G)$ est donc un sous-groupe compact de $GL(\mathcal{S}_n(\mathbb{R}))$. L'ensemble $\mathcal{S}_n^{++}$ étant convexe, on a $\text{Conv}(\{AA^T \mid A \in G\}) \subset \mathcal{S}_n^{++}$. De plus, $\{AA^T \mid A \in G\}$ est stable par $G$ donc $\text{Conv}(\{AA^T \mid A \in G\})$ aussi et d'après le théorème de Kakutani, il existe un point fixe $B \in \mathcal{S}_n^{++}$ pour l'action de $G$. Si $C \in \mathcal{S}_n^{++}$ vérifie $C^2 = B$, on a alors

$$\forall A \in G,\ AC^2A^T = C^2$$

donc

$$\forall A \in G,\ C^{-1}AC(C^{-1}AC)^T = I$$

ce qui signifie que $C^{-1}GC \subset O(n,\mathbb{R})$.

# Décomposition polaire de $O(p,q)$

## Cadre :

La décomposition polaire induit un homéomorphisme $O(p,q) \simeq O(p) \times O(q) \times \mathbb{R}^{pq}$.

**Recasages** :

- 

**Référence** : NH2G2 tome 1.

## Développement :

Les étapes sont :

1. Montrer que $O(p,q)$ est stable par transposée,
2. Montrer que la décomposition polaire induit $O(p,q) \simeq (O(p,q) \cap O(n)) \times (O(p,q) \cap S_n^{++}(\mathbb{R}))$,
3. Déterminer $O(p,q) \cap O(n)$ et $O(p,q) \cap S_n^{++}(\mathbb{R})$.

**Étape 1 :** Par définition, on a

$$O(p,q) = \{A \in M_n(\mathbb{R}) \mid A^t J A = J\}$$

donc

$$\begin{aligned} A \in O(p,q) &\implies A^t J A = J \\ &\implies A^t J A = J \\ &\implies A^{-1} J (A^t)^{-1} = J \\ &\implies (A^t)^{-1} \in O(p,q) \\ &\implies A^t \in O(p,q). \end{aligned}$$

**Étape 2 :** Soit $M \in O(p,q)$. Posons $M = OS$ sa décomposition polaire et $A = M^t M$. On a alors $A \in O(p,q) \cap S_n^{++}(\mathbb{R})$ et $A = S^2$. Montrons que $S \in O(p,q)$. Pour cela, posons $U \in S_n(\mathbb{R})$ l'unique matrice telle que $A = \exp U$. On a alors $S = \exp(U/2)$ et donc

$$\begin{aligned} A \in O(p,q) &\iff A^t J A = J \\ &\iff A^t = J A^{-1} J^{-1} \\ &\iff \exp U^t = J \exp(-U) J^{-1} \\ &\iff \exp U^t = \exp\left(-JUJ^{-1}\right) \\ &\iff U^t = -JUJ^{-1} \\ &\iff U^t J + JU = 0 \\ &\iff \frac{U^t}{2} J + J \frac{U}{2} = 0 \\ &\iff \exp \frac{U}{2} \in \mathrm{O}(p,q) \\ &\iff S \in O(p,q). \end{aligned}$$

Ainsi, $S \in O(p,q)$ et $O = AS^{-1} \in O(p,q)$ donc la décomposition polaire induit bien un tel homéomorphisme.

**Étape 3 :** Soit $M \in O(p,q) \cap O(n)$. Posons

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

On a d'une part

$$I = M^t M = \begin{pmatrix} A^t & C^t \\ B^t & D^t \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A^t A + C^t C & A^t B + C^t D \\ B^t A + D^t C & B^t B + D^t D \end{pmatrix}$$

et d'autre part

$$J = M^t J M = \begin{pmatrix} A^t & C^t \\ B^t & D^t \end{pmatrix} J \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A^t & C^t \\ B^t & D^t \end{pmatrix} \begin{pmatrix} -A & -B \\ C & D \end{pmatrix}$$

$$= \begin{pmatrix} -AA^t + C^tC & -A^tB + C^tD \\ -B^tA + D^tC & -B^tB + D^tD \end{pmatrix}.$$

Ainsi, $C^tC = 0$, $D^tD = 0$, $A^tA = I$, $D^tD = I$ donc $M \in O(p) \times O(q)$.
D'après l'étape 2, si l'exponentielle induit un homéomorphisme entre $O(p,q) \cap S_n^{++}(\mathbb{R})$ et

$$L := \{M \in S_n(\mathbb{R}) \mid MJ + JM = 0\}.$$

Ainsi, on a $O(p,q) \cap S_n^{++}(\mathbb{R}) \simeq L \simeq \mathbb{R}^{pq}$ car $L$ est un $\mathbb{R}$-espace vectoriel de dimension $pq$. En effet, l'équation

$$MJ + JM = 0$$

implique que

$$L = \left\{ \begin{pmatrix} 0 & C \\ C^t & 0 \end{pmatrix} \mid C \in M_{p,q}(\mathbb{R}) \right\}.$$

# Forme de Hankel

## Cadre :

Soit $P$ un polynôme à coefficients réels dont les racines distinctes sont $x_1, \dots, x_t$ avec multiplicités $m_1, \dots, m_t$. Pour $k \in \mathbb{N}$, on pose

$$s_k = \sum_{i=1}^{t} m_i x_i^k.$$

La forme quadratique réelle $q(X) = \sum_{i,j} s_{i+j-2} X_i X_j$ est alors de signature $(\frac{t+r}{2}, \frac{t-r}{2})$ où $r$ est le nombre de racines réelles de $P$.

**Recasages** :

- 

**Référence** : NH2G2 tome 1.

## Développement :

Les étapes sont :

1. Justifier que $q$ est une forme quadratique réelle.
2. Montrer que les $\phi_k(X) = \sum_{i=1}^{n} x_k^{i-1} X_i$ sont des formes linéaires indépendantes sur $\mathbb{C}$.
3. Montrer que $q = \sum_{i=1}^{t} m_i \phi_i^2$.
4. Conclure.

**Étape 1 :** $q$ est un polynôme homogène de degré 2 donc il suffit de montrer que ses coefficients sont réels. Or, ses coefficients sont des polynômes symétriques en les racines de $P$ et $P$ est à coefficients réels donc le théorème fondamental sur les polynômes symétriques implique que les coefficients de $q$ sont réels.

**Étape 2 :** La matrice de $(\phi_1, \dots, \phi_t)$ dans la base duale de la base canonique de $\mathbb{C}^n$ est

$$\begin{pmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_t \\ x_1^2 & \cdots & x_t^2 \\ \vdots & & \vdots \\ x_1^{n-1} & \cdots & x_t^{n-1} \end{pmatrix}.$$

La matrice carrée extraite à partir des $t$ premières lignes est une matrice de Vandermonde et les $x_i$ sont distincts donc elle est inversible et la matrice initiale est de rang $t$, d'où l'indépendance linéaire des $\phi_i$ sur $\mathbb{C}$.

**Étape 3 :** On a

$$\begin{aligned} \sum_{k=1}^{t} m_k \phi_k^2 &= \sum_{k=1}^{t} \sum_{i,j} x_k^{i+j-2} X_i X_j \\ &= \sum_{i} \left( \sum_{k=1}^{t} m_k x_k^{2i-2} \right) X_i^2 + \sum_{i<j} 2 \left( \sum_{k=1}^{t} m_k x_k^{i+j-2} \right) X_i X_j \\ &= q. \end{aligned}$$

Posons $I = \{i \in [\![1,t]\!] \mid x_i \in \mathbb{R}\}$ et $J = \{i \in [\![1,t]\!] \mid x_i \notin \mathbb{R}\}$. $P$ étant à coefficients réels, si $i \in J$, il existe $j \in J, j \neq i$ tel que $\overline{x_i} = x_j$ et on a de plus $m_i = m_j$. En regroupant ces deux termes, on trouve (sur $\mathbb{R}^n$) :

$$\begin{aligned} m_i \phi_i^2 + m_j \phi_j^2 &= m_i (\phi_i^2 + \overline{\phi_i}^2) \\ &= 2 \operatorname{Re}(\phi_i)^2 - 2 \operatorname{Im}(\phi_i)^2. \end{aligned}$$

Les formes $\phi_i$ et $\phi_j$ étant linéairement indépendantes sur $\mathbb{C}$, le rang de $m_i \phi_i^2 + m_j \phi_j^2$ est 2 donc $\operatorname{Re}(\phi_i)^2$ et $\operatorname{Im}(\phi_i)^2$ sont linéairement indépendantes sur $\mathbb{C}$ et donc sur $\mathbb{R}$ aussi puisque le rang est invariant par extension. Finalement, $m_i \phi_i^2 + m_j \phi_j^2$ est une forme quadratique réelle de rang $(1,1)$.
En regroupant les $m_i \phi_i^2$ correspondants aux $r$ racines réelles de $P$ et en regroupant deux-à-deux les $m_i \phi_i^2$ correspondants aux racines non réelles de $P$, on obtient une mise au carré de $q$ à partir de formes linéaires réelles linéairement indépendantes. Ainsi, la signature de $q$ est $(r,0) + \frac{t-r}{2}(1,1) = (\frac{t+r}{2}, \frac{t-r}{2})$.

# 26 est le seul entier entre un carré et un cube

## Cadre :

Les seules solutions entières à $x^2 + 2 = y^3$ sont $(\pm 5, 3)$.

**Recasages** :

- 

**Référence** :

## Développement :

Les étapes sont :

1. Montrer que $\mathbb{Z}[i\sqrt{2}]$ est euclidien et déterminer ses unités,
2. Montrer que $x + i\sqrt{2} \wedge x - i\sqrt{2} = 1$ dans $\mathbb{Z}[i\sqrt{2}]$,
3. Conclure.

1. Considérons le stathme $N : a + ib\sqrt{2} \mapsto a^2 + 2b^2$ défini sur $\mathbb{Z}[i\sqrt{2}]$. Déterminons d'abord les inversibles de $\mathbb{Z}[i\sqrt{2}]$. Comme $N$ est à valeurs dans $\mathbb{N}$, on a $\mathbb{Z}[i\sqrt{2}]^\times = N^{-1}(\{1\})$. Soient donc $a, b \in \mathbb{Z}$ tels que $a^2 + 2b^2 = 1$. On a nécessairement $b = 0$ donc $a = \pm 1$. Ainsi, $\mathbb{Z}[i\sqrt{2}]^\times = \{\pm 1\}$.

   Montrons que $\mathbb{Z}[i\sqrt{2}]$ est euclidien. Soient $a + i\sqrt{2}b, c + i\sqrt{2}d \in \mathbb{Z}[i\sqrt{2}]$. On pose $\frac{a+i\sqrt{2}b}{c+i\sqrt{2}d} = e + i\sqrt{2}f \in \mathbb{Q}[i\sqrt{2}]$. Fixons $n, m \in \mathbb{Z}$ tels que

   $$|n - e| \leqslant \frac{1}{2}, \qquad |m - f| \leqslant \frac{1}{2}.$$

   Alors, on a $a + i\sqrt{2}b = (c + i\sqrt{2}d)(n + i\sqrt{2}m) + r$ avec

   $$\begin{aligned} N(r) &= N(c + i\sqrt{2}d)N(e + i\sqrt{2}f - n + i\sqrt{2}m) \\ &= N(c + i\sqrt{2}d)\Big((e - n)^2 + 2(f - m)^2\Big) \\ &\leqslant N(c + i\sqrt{2}d)\Big(\frac{1}{4} + 2\frac{1}{4}\Big) \\ &< N(c + i\sqrt{2}d). \end{aligned}$$

2. Soit $d$ un diviseur commun de $x + i\sqrt{2}$ et $x - i\sqrt{2}$ dans $\mathbb{Z}[i\sqrt{2}]$. On a alors $d \mid 2i\sqrt{2}$. Or, $i\sqrt{2}$ est irréductible dans $\mathbb{Z}[i\sqrt{2}]$ (car sa norme est un nombre premier) donc les diviseurs de $2i\sqrt{2} = -(i\sqrt{2})^3$ sont au signe près les $(i\sqrt{2})^k$, $k = 0, 1, 2, 3$. Si $i\sqrt{2}$ était un diviseur de $x + i\sqrt{2}$ alors on aurait

   $$\frac{x + i\sqrt{2}}{i\sqrt{2}} = \frac{2 - i\sqrt{2}x}{2} \in \mathbb{Z}[i\sqrt{2}]$$

   et donc $x$ serait pair. Or, $x$ pair implique $y^3$ pair et donc $y^3$ multiple de 8 mais $x^2 + 2$ n'est pas multiple de 4. Ainsi, $x + i\sqrt{2} \wedge x - i\sqrt{2} = 1$ dans $\mathbb{Z}[i\sqrt{2}]$.
3. Fixons $(x, y)$ une solution. On a alors

   $$(x + i\sqrt{2})(x - i\sqrt{2}) = y^3$$

   et les deux termes du membre de gauche sont premiers entre eux donc ce sont chacun des cubes dans $\mathbb{Z}[i\sqrt{2}]$. Posons $a, b \in \mathbb{Z}$ tels que $x + i\sqrt{2} = (a + i\sqrt{2}b)^3$. On a alors

   $$x + i\sqrt{2} = (a + i\sqrt{2}b)^3 = a^3 + 3a^2 i\sqrt{2}b + 3a(-2)b^2 - 2i\sqrt{2}b^3$$

   d'où

   $$3a^2 b - 2b^3 = 1$$

   et $b = \pm 1$. Si $b = 1$, on a $3a^2 = 3$ donc $a = \pm 1$ et si $b = -1$ alors $-3a^2 = 3$ ce qui est impossible. Ainsi, on a $(a, b) \in \{(1, 1), (-1, 1)\}$ et donc $x = \pm 5$ ce qui permet de conclure.

# Homéomorphisme entre $S_n$ et $S_n^{++}$, racine carrée et décomposition polaire

## Cadre :

On montre que l'exponentielle induit un homéomorphisme entre $S_n$ et $S_n^{++}$. On applique ensuite ce résultat à la racine carrée et à la décomposition polaire.

**Recasages** :

- 

**Référence** :

## Développement :

Les étapes sont :

1. On montre que exp est surjective.
2. On montre que exp est injective.
3. On montre que log est continue.
4. On montre que $\sqrt{}$ est bien définie et continue.
5. On montre que la décomposition polaire est un homéomorphisme.

1. Soit $B \in S_n^{++}$. Par le théorème spectral, si $\lambda_1, \dots, \lambda_n > 0$ sont les valeurs propres de $B$, il existe $P \in O(n, \mathbb{R})$ telle que $B = P\text{diag}(\lambda_1, \dots, \lambda_n)P^{-1}$. On a alors $B = \exp A$ avec
$$A = P\text{diag}(\ln \lambda_1, \dots, \ln \lambda_n)P^{-1} \in S_n.$$
2. Soient $A, B \in S_n$ telles que $\exp A = \exp B$. On diagonalise $A$ :
$$A = P\text{diag}(\lambda_1, \dots, \lambda_n)P^{-1}.$$
Comme $\exp A = P\text{diag}(\lambda_1, \dots, \lambda_n)P^{-1}$, $A$ est un polynôme en $\exp A$ et donc en $\exp B$ et donc en $B$. Ainsi, $A$ et $B$ commutent et on peut les codiagonaliser. En inspectant les valeurs propres, on trouve $A = B$.
3. Fixons $(B_n)_{n\in\mathbb{N}} \in {S_n^{++}}^{\mathbb{N}}$ une suite convergente vers $B \in S_n^{++}$. La convergence de la suite $(B_n)$ implique que les valeurs propres de ces matrices sont un intervalle $[a, b]$ avec $a, b > 0$ (formule rayon spectral). En particulier, $(\log B_n)_n$ est une suite du compact donné par l'image de
$$\begin{array}{ccc} [\ln a, \ln b]^n \times O(n) & \to & S_n^{++} \\ (\lambda_1, \dots, \lambda_n, P) & \mapsto & P\text{diag}(\lambda_1, \dots, \lambda_n)P^{-1} \end{array}$$
donc il suffit de montrer qu'elle n'admet qu'une seule valeur d'adhérence. Soit $A \in S_n$ une telle valeur d'adhérence et $\varphi$ telle que $\log B_{\varphi(n)} \mapsto A$. On a alors
$$\exp A = \lim \exp \log B_{\varphi(n)} = \lim B_{\varphi(n)} = B$$
donc $A = \log B$.
4. Si $A, B \in S_n^{++}$, on a
$$A = B^2 \iff \log A = \log\big(B^2\big) \iff \log A = 2 \log B \iff B = \exp\Big(\frac{1}{2} \log A\Big)$$
donc l'application $\sqrt{}$ est bien définie et est donnée par
$$\sqrt{A} = \exp\Big(\frac{1}{2} \log A\Big)$$
donc c'est un homéomorphisme de $S_n^{++}$ sur lui-même.
5. La réciproque de la décomposition polaire est en fait donnée par
$$\begin{array}{ccc} \text{GL}(n, \mathbb{R}) & \to & O(n) \times S_n^{++} \\ M & \mapsto & (M\sqrt{M^T M}^{-1}, \sqrt{M^T M}) \end{array}$$
donc c'est bien un homéomorphisme.

# Construction des corps finis

## Cadre :

On montre que pour tout $q = p^n$, il existe un unique corps fini de cardinal $q$. On démontre ensuite que son groupe des inversibles est cyclique pour en déduire une construction plus explicite à partir de polynômes.

**Recasages** :

- 

**Référence** :

## Développement :

Les étapes sont :

1. On montre que l'ensemble des racines de $X^q - X$ dans $\overline{\mathbb{F}_p}$ est un corps de cardinal $q$ puis que c'est le seul.
2. On montre que $\mathbb{F}_q^*$ est cyclique.
3. On en déduit l'existence d'un polynôme irréductible de degré $n$ sur $\mathbb{F}_p$ pour tout $n$ et tout $p$.

1. Posons $\mathbb{F}_q = \{x \in \overline{\mathbb{F}_p} \mid x^q = x\}$. L'application $x \mapsto x^p$ étant un morphisme d'anneaux en caractéristique $p$, l'application $x \mapsto x^q$ l'est aussi et on a :

$$\forall x, y \in \mathbb{F}_q, \begin{cases} (x-y)^q = x^q - y^q = x - y, \\ (xy)^q = x^q y^q = xy, \\ (x^{-1})^q = (x^q)^{-1} = x^{-1} \text{ si } x \neq 0, \end{cases}$$

$$0^q = 0,$$

$$1^q = 1.$$

   Ainsi, $\mathbb{F}_q$ est un corps et il est de cardinal $q$ car $X^q - X$ est à racines simples :

$$(X^q - X)' = qX^{q-1} - 1 = -1$$

   n'a pas de racine.
   Montrons que c'est le seul corps de cardinal $q$. Si $\mathbb{K}$ est un corps de cardinal $q$, le théorème de Lagrange implique que

$$\forall x \in \mathbb{K}^*, \quad x^{q-1} = 1$$

   donc $\mathbb{K}$ est inclus dans $\mathbb{F}_q$ donc égal à $\mathbb{F}_q$.
2. Introduisons la fonction indicatrice d'Euler

$$\varphi : n \mapsto \text{Card}(\{k \in \mathbb{N}^* \mid k \wedge n = 1\}).$$

   Si $k \in \mathbb{N}^*$, $\varphi(k)$ est le nombre d'éléments d'ordre $k$ dans $\mathbb{Z}/n\mathbb{Z}$. On en déduit la formule

$$\forall n \in \mathbb{N}^*, \qquad \sum_{d|n} \varphi(d) = n.$$

   Pour tout $d \mid q-1$, notons $\psi(d)$ le nombre d'élément d'ordre $d$ de $\mathbb{F}_q^*$. Si $d \mid q-1$ et $x \in \mathbb{F}_q^*$ est $x$ est d'ordre $d$ alors $\langle x \rangle$ est précisément l'ensemble des racines de $X^d - 1$ dans $\mathbb{F}_q$ donc tout élément d'ordre $d$ de $\mathbb{F}_q^*$ est dans $\langle x \rangle$. En particulier, $\psi(d) = \phi(d)$.
   Ainsi, $\psi(d) \in \{0, \phi(d)\}$ pour tout $d \mid q-1$. Si $\psi(q-1) \neq \phi(q-1)$ alors on a

$$q - 1 = \sum_{d|q-1} \psi(d) < \sum_{d|q-1} \phi(d) = q - 1$$

   ce qui est absurde.
3. Soit $\alpha \in \mathbb{F}_q^*$ un générateur de $\mathbb{F}_q^*$. Alors, $\mathbb{F}_q = \mathbb{F}_p(\alpha)$ donc le polynôme minimal de $\alpha$ sur $\mathbb{F}_p$ est irréductible de degré $n$ et on peut construire $\mathbb{F}_q$ comme

$$\mathbb{F}_q \simeq \mathbb{F}_p[X]/\langle \pi_{\alpha,\mathbb{F}_p} \rangle.$$

# Théorème de Wantzel

## Cadre :

On montre qu'un nombre $\alpha \in \mathbb{R}$ est constructible à la règle et au compas si et seulement si il existe une tour d'extensions

$$\mathbb{Q} = \mathbb{K}_0 \subset \cdots \subset \mathbb{K}_n \ni \alpha$$

avec $[\mathbb{K}_{i+1} : \mathbb{K}_i] = 2$.

**Recasages** :

- 

**Référence** :

## Développement :

**Implication :**
Supposons que $\alpha = (x, y)$ soit constructible à partir de $\mathcal{P}$. Posons $\mathbb{K}$ l'extension de $\mathbb{Q}$ engendrée par et les coordonnées des points de $\mathcal{P}$. Par définition, $\alpha$ est un point d'intersection de deux droites ou d'une droite et d'un cercle ou de deux cercles.

1. Si $\alpha$ est un point d'intersection de deux droites : il existe $a, b, c, a', b', c' \in \mathbb{K}$ tels que

$$ax + by + c = 0, \quad a'x + b'y + c' = 0, \quad \begin{vmatrix} a & a' \\ b & b' \end{vmatrix} \neq 0.$$

   On peut alors utiliser l'une des équations pour exprimer $x$ affinement en fonction de $y$ (ou l'inverse) puis la seconde équation montrer que $y$ vérifie une équation linéaire dans $\mathbb{K}$. Ainsi, $x \in \mathbb{K}$ et $y$ aussi grâce aux équations.

2. Si $\alpha$ est un point d'intersection d'une droite et d'un cercle : comme précédemment, on peut écrire $x = ay+b$ ou $y = ax+b$ et réinjecter dans l'équation du cercle, ce qui implique que $x$ (ou $y$) est solution d'une équation de degré 2 à coefficients dans $\mathbb{K}$. On en déduit que $y \in \mathbb{K}$ (ou $x \in \mathbb{K}$) grâce à la relation linéaire entre les deux.

3. Si $\alpha$ est un point d'intersection de deux cercles distincts. Alors, $(x, y)$ vérifient

$$(x - a_1)^2 + (y - b_1)^2 = r_1^2, \quad (x - a_2)^2 + (y - b_2)^2 = r_2^2.$$

   En soustrayant la première équation à la première, on trouve

$$2(a_1 - a_2)x + 2(b_1 - b_2)y + a_2^2 - a_1^2 + b_2^2 - b_1^2 = r_2^2 - r_1^2$$

   donc on est ramené dans le premier cas.

Dans tous les cas, $\mathbb{K}(\alpha)$ est une extension de degré 1 ou 2 de $\mathbb{K}$ donc on peut en conclure l'implication par récurrence.

**Réciproque :** Pour la réciproque, nous allons montrer que le corps Ł des nombres constructibles est stable par racine carrée positive. Pour cela, on applique le théorème de Pythagore au triangle rectangle inscrit dans le cercle dont un diamètre est donné par le segment d'extrémités $(-1, 0)$, $(a, 0)$. Fixons alors un $\alpha \in \mathbb{R}$ tel qu'il existe une tour d'extensions

$$\mathbb{Q} = L_0 \subset \cdots \subset L_n \ni \alpha.$$

Montrons par récurrence que $L_i \subset k$ pour tout $i$.
**Initialisation :** $L_0 = Q \subset k$.

**Hérédité :** Supposons $L_i \subset k$ et fixons $\beta \in \mathbb{R}$ tel que $L_{i+1} = L_i(\beta)$. Le polynôme minimal de $\beta$ sur $L_i$ est de degré 2 donc il existe $a, b \in L_i$ tels que $\beta^2 + a\beta + b = 0$. On a alors $\beta = \frac{-b \pm \sqrt{b^2 - 4c}}{2} \in k$ avec $b^2 - 4c > 0$ car ce polynôme admet une racine réelle.

# Décomposition de Dunford

## Cadre :

On démontre le lemme des noyaux et la décomposition de Dunford.

**Recasages** :

- 

**Référence** :

## Développement :

**Lemme des noyaux :** Posons $P = \prod_{i=1}^{r} P_i^{\alpha_i}$ la décomposition de $P$ en irréductibles. Pour tout $j$, posons $Q_j = \prod_{i=1, i\neq j}^{r} P_i^{\alpha_i}$. Les $Q_j$ sont premiers entre-eux dans leur ensemble donc il existe $U_1, \dots, U_r$ tels que

$$U_1 Q_1 + \cdots + U_r Q_r = 1.$$

Posons $\pi_i = U_i Q_i(u)$. On a donc

$$\pi_1 + \cdots + \pi_r = \mathrm{id}\,.$$

De plus, $P \mid Q_i Q_j$ si $i \neq j$ donc $\pi_i \pi_j = 0$ et il suit que

$$\pi_i^2 = \pi_i(\mathrm{id} - \sum_{j=1, j\neq i}^{r} \pi_j) = \pi_i.$$

Ainsi, les $p_i$ sont une famille de projecteurs orthogonaux deux-à-deux et dont la somme fait id. Il suffit donc de montrer que l'image de $\pi_i$ est $\ker P_i^{\alpha_i}(u)$.
Soit $x \in \ker P_i^{\alpha_i}(u)$. On a alors

$$x = \sum_{j=1}^{r} \pi_j(x) = \pi_i(x) \in \mathrm{Im}(\pi_i)$$

car $P_i^{\alpha_i} \mid Q_j$ dès que $i \neq j$. Réciproquemet, si $x \in \mathrm{Im}(\pi_i)$ et $y \in E$ vérifie $\pi_i(y) = x$ alors on a

$$P_i(x) = U_i P_i Q_i(u)(x) = U_i P(u)(x) = 0.$$

**Décomposition de Dunford :** Posons $P = \prod_{i=1}^{r} (X - \lambda_i)^{n_i}$ le polynôme caractéristique de $u$. Le lemme des noyaux implique la décomposition

$$E = \bigoplus_{i=1}^{r} E_i$$

où les $E_i$ sont les sous-espaces caractéristiques de $u$. De plus, le lemme des noyaux nous assure que les projecteurs $\pi_i$ associés sont des polynômes en $u$. Posons $d = \lambda_1 \pi_1 + \cdots + \lambda_r \pi_r$ et $n = u - d$. On a alors $d + n = u$ et $d$ et $n$ sont des polynômes en $u$ donc commutent. De plus, la matrice de $d$ dans une base adaptée à la décomposition précédente est diagonale donc $d$ est diagonalisable et $n_{|E_i}$ est nilpotent pour tout $i$ donc $n$ est nilpotent. Ceci prouve l'existence de la décomposition de Dunford.
Soit $u = d' + n'$ une autre décomposition de Dunford. $d'$ commute avec $n'$ donc avec $u$ et donc avec $d$ car $d$ est un polynôme en $u$. De même, $n'$ commute avec $n$. Ainsi, $d$ et $d'$ sont codiagonalisables donc $d - d'$ est diagonalisable et $n' - n$ est nilpotent. Or, on a

$$d - d' = n' - n$$

donc $d - d'$ est diagonalisable nilpotent d'où $d - d' = 0$ et il suit que $d = d'$, $n = n'$ d'où l'unicité de la décomposition de Dunford.

# Dénombrement des polynômes irréductibles unitaires sur $\mathbb{F}_q$

## Cadre :

On montre que $I(n,q) \sim \frac{q^n}{n}$.

**Recasages** :

- 

**Référence** :

## Développement :

Les étapes sont :

1. On montre $X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}_d} P$.
2. On montre la formule d'inversion de Möbius : si $g = \sum_{d|n} f(d)$ alors $f = \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right)$.
3. On conclut.

1. Remarquons déjà que $X^{q^n} - X$ est sans multiplicité car son dérivé est $-1$. Soit $P$ un diviseur irréductible de $X^{q^n} - X$ de degré $d$ et soit $\alpha$ une racine de $P$. L'extension de $\mathbb{F}_q$ engendrée par $\alpha$ est de degré $d$ donc $\mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$ et $d \mid n$. Réciproquement, si $d \mid n$ et $P$ est un polynôme irréductible unitaire de degré $d$ sur $\mathbb{F}_q$ et si $\alpha$ est une racine de $P$ alors $\alpha \in \mathbb{F}_{q^n}$ puisque $\alpha \in \mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$ et donc $P \mid X^{q^n} - X$.
2. Si $n \in \mathbb{N}$, on a
$$\begin{aligned}\sum_{d|n} g\left(\frac{n}{d}\right)\mu(d) &= \sum_{d|n} \sum_{d' \mid \frac{n}{d}} f(d')\mu(d) \\ &= \sum_{dd'|n} f(d')\mu(d) \\ &= \sum_{d'|n} f(d') \sum_{d \mid \frac{n}{d'}} \mu(d) \\ &= f(n).\end{aligned}$$
On a ici utilisé la formule
$$\sum_{d|n} \mu(d) = \begin{cases} 1 \text{ si } n = 1, \\ 0 \text{ sinon.} \end{cases}$$
En effet, si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} > 1$, on a
$$\begin{aligned}\sum_{d|n} \mu(d) &= \sum_{s=0}^{r} \sum_{1 \leqslant i_1 < \cdots < i_s \leqslant r} \mu(p_{i_1} \cdots p_{i_s}) \\ &= \sum_{s=0}^{r} \binom{r}{s} (-1)^s \\ &= (1-1)^r \\ &= 0.\end{aligned}$$
3. D'après la première formule, on a
$$q^n = \sum_{d|n} dI(d,q)$$
donc la formule d'inversion de Möbius implique que
$$nI(n,q) = \sum_{d|n} q^d \mu\left(\frac{n}{d}\right)$$
et donc
$$I(n,q) \underset{q \to +\infty}{\sim} \frac{q^n}{n}.$$

# Théorème de Wedderburn

## Cadre :

On montre que tout corps gauche fini est commutatif.

**Recasages** :

- 

**Référence** :

## Développement :

Démontrons tout d'abord que

$$X^n - 1 = \prod_{d|n} \Phi_d.$$

Pour ça, on regroupe les racines de l'unité suivant leur ordre :

$$\begin{aligned} X^n - 1 &= \prod_{\zeta \in \mathbb{U}_n} (X - \zeta) \\ &= \prod_{d|n} \prod_{\zeta \in \mathbb{U}_d^*} (X - \zeta) \\ &= \prod_{d|n} \Phi_d. \end{aligned}$$

Montrons maintenant que si $q \geqslant 2$ et $d, n \in \mathbb{N}$, on a

$$q^d - 1 \mid q^n - 1 \implies d \mid n.$$

Fixons de tels entiers et posons $n = dr + s$ la division euclidienne de $n$ par $d$. On a alors

$$q^n - 1 = (q^d - 1)(q^{n-d} + q^{n-2d} + \cdots + q^{d+s} + q^s) + q^s - 1$$

d'où $q^d - 1 \mid q^s - 1$ mais $0 \leqslant s < d$ donc $0 \leqslant q^s - 1 < q^d - 1$ et donc $s = 0$. Ainsi, $d \mid n$.
Fixons maintenant un corps gauche fini $k$. Pour $y \in k^*$, on pose aussi

$$k_y = \{x \in k \mid xy = yx\}.$$

Enfin, on pose $k' = Z(k)$ et $q = |k'|$. Remarquons que $k'$ est un sous-corps de $k$ : il contient le sous-corps premier de $k$. Comme $k$ est un espace vectoriel sur $k'$, il existe $n \in \mathbb{N}^*$ tel que $|k| = q^n$. De même, si $y \in k$, $k_y$ est un corps gauche contenant $k'$ donc il existe $d_y \geqslant 1$ tel que $|k_y| = q^{d_y}$. Supposons $k$ non commutatif, c'est-à-dire $n > 1$. On fait agir $k^*$ sur lui même par conjugaison. Si $x_1, \ldots, x_r$ sont des représentants des orbites non ponctuelles $\omega(x_1), \ldots, \omega(x_r)$, l'équation aux classes donne

$$q^n - 1 = q - 1 + \sum_i \frac{q^n - 1}{q^{d_{x_i}} - 1}.$$

De plus, pour tout $i$, $x_i \notin k'$ donc $d_{x_i} < n$. Ainsi, comme la formule précédente implique que

$$q^n - 1 = \prod_{d|n} \Phi_d(q)$$

et comme $d_{x_i} \mid n$ pour tout $i$ (car $q^{d_{x_i}} - 1 \mid q^n - 1$), on a

$$\frac{q^n - 1}{q^{d_{x_i}} - 1} = \prod_{d|n, d \nmid d_{x_i}} \Phi_d(q) \in \Phi_n(q)\mathbb{Z}.$$

Par somme, on en déduit que $\Phi_n(q) \mid q - 1$. Or, comme $n > 1$, $\mathbb{U}_n^* \backslash \{1\} \neq \emptyset$ donc

$$|\Phi_n(q)| = \left| \prod_{\zeta \in \mathbb{U}_n^*} (q - \zeta) \right| > q - 1$$

ce qui contredit $\Phi_n(q) \mid q - 1$.

# Théorème de Cauchy-Lipschitz linéaire

## Cadre :

On montre que si $I$ est un intervalle de $\mathbb{R}$ et $A \in C(I, M_n(\mathbb{R}))$, $B \in C(I, \mathbb{R}^n)$, $t_0 \in I$, $y_0 \in \mathbb{R}^n$, il existe une unique solution $C^1$ au problème de Cauchy

$$\begin{cases} y'(t) = A(t)y(t) + B(t), \\ y(t_0) = y_0. \end{cases}$$

**Recasages** :

- 

**Référence** :

Équations différentielles - Berthelin

## Développement :

Commençons par reformuler le problème de Cauchy sous forme intégrale. Pour cela, on remarque que le théorème fondamental de l'analyse implique que si $y$ est une solution alors

$$y(t) = y_0 + \int_{t_0}^{t} A(s)y(s) + B(s)\mathrm{d}s.$$

Le théorème fondamental de l'analyse nous donne également une réciproque : $y$ est solution du problème de Cauchy si et seulement si $y$ est continue et vérifie l'équation intégrale ci-dessus. On se ramène donc à la recherche d'un point fixe pour une application linéaire dans $C(I, \mathbb{R}^n)$.

Supposons tout d'abord $I$ compact. Posons $E = C(I, \mathbb{R}^n)$, $\alpha = \inf I + t_0$, $\beta = \sup I - t_0$ et

$$\Phi : \begin{array}{ccc} E & \to & E \\ y & \mapsto & t \mapsto y_0 + \int_{t_0}^{t} A(s)y(s) + B(s)\mathrm{d}s \end{array}.$$

Remarquons que $\Phi$ est bien définie. Soient $y, \tilde{y} \in E$. Montrons par récurrence que pour tout $p \in \mathbb{N}$ et tout $t \in I$, on a

$$|\Phi^p(y)(t) - \Phi^p(\tilde{y})(t)| \leqslant \frac{k^p |t - t_0|^p}{p!} \|y - \tilde{y}\|$$

où $k = \sup_{s \in I} \|A(s)\|$.

**Initialisation :** Pour tout $t \in I$, on a

$$|\Phi^0(y)(t) - \Phi^p(\tilde{y})(t)| = |y(t) - \tilde{y}(t)| \leqslant \|y - \tilde{y}\|.$$

**Hérédité :** Soit $p \in \mathbb{N}$ tel que la propriété soit vraie au rang $p$. Pour tout $t \geqslant t_0$ on a

$$\begin{aligned} |\Phi^{p+1}(y)(t) - \Phi^{p+1}(y)(t)| &= \left| \int_{t_0}^{t} A(s)(\Phi^p(y)(s) - \Phi^p(\tilde{y})(t))\mathrm{d}s \right| \\ &\leqslant \int_{t_0}^{t} k \frac{k^p (s - t_0)^p}{p!} \|y - \tilde{y}\| \mathrm{d}s \\ &= \frac{k^{p+1}(t - t_0)^{p+1}}{(p+1)!} \|y - \tilde{y}\|. \end{aligned}$$

On procède de même si $t \leqslant t_0$.

En posant $\gamma = \max(|\alpha|, |\beta|)$, on a donc pour tout $p \in \mathbb{N}$

$$\forall t \in I, \quad |\Phi^p(y)(t) - \Phi^p(\tilde{y})(t)| \leqslant \frac{k^p \gamma^p}{p!} \|y - \tilde{y}\|$$

et en passant à la borne supérieure

$$\|\Phi^p(y) - \Phi^p(\tilde{y})\| \leqslant \frac{k^p \gamma^p}{p!} \|y - \tilde{y}\|.$$

La série de terme général positif $\frac{k^p\gamma^p}{p!}$ étant converge, son terme général tend vers 0 et il existe $m \in \mathbb{N}$ tel que $\frac{k^p\gamma^p}{p!} \in [0,1[$. L'inégalité précédente implique alors que $\Phi^m$ est une contraction de l'espace métrique complet $E$, ce qui implique par le théorème du point fixe de Picard que $\Phi$ admet un unique point fixe dans $E$. Ainsi, il existe bien une unique solution au problème de Cauchy initial.

Si $I$ n'est pas compact, on applique ce qui précède à une suite d'intervalles compacts $I_n$ tels que $I = \cup_n I_n$. On obtient alors une suite de fonctions $(y_n)_n$ définies respectivement sur $(I_n)_n$ et on pose

$$y : \begin{array}{ccc} I & \to & \mathbb{R}^n \\ t & \mapsto & y_n(t) \text{ si } t \in I_n. \end{array} .$$

L'unicité des solutions sur les $I_n$ impliquent que $y$ est bien définie et est l'unique solution au problème de Cauchy.

# $\mathbb{C}^*$ n'est pas simplement connexe

## Cadre :

On montre que l'intégration des fonctions holomorphes est invariante par homotopie et on en déduit que $\mathbb{C}^*$ n'est pas simplement connexe.

**Recasages** :

- 

**Référence** :

Analyse complexe - Jacques Douchet

## Développement :

Fixons $\Omega$ un domaine de $\mathbb{C}$ et $\gamma_0, \gamma_1$ deux courbes $C^1$ par morceaux homotopes d'extrémités $a, b \in \Omega$. Posons $H : [0,1]^2 \to \Omega$ l'homotopie associée. $H$ est donc continue et vérifie

$$H(0,\cdot) = \gamma_0, \qquad H(1,\cdot) = \gamma_1, \qquad H(s,0) = a, \qquad H(s,1) = b.$$

Pour $s \in [0,1]$, on notera $\gamma_s = H(s,\cdot)$. $H$ étant continue, $K := H([0,1]^2)$ est un compact de $\Omega$ donc il existe $r > 0$ tel que

$$\forall x \in \Omega, \quad B(x, 6r) \subset \Omega.$$

Chaque chemin $\gamma_s$ $(0 < s < 1)$ étant continue sur un compact, le théorème de Heine permet de construire des chemins polygonaux $\tilde{\gamma}_s$ vérifiant

$$\|\gamma_s - \tilde{\gamma}_s\| \leqslant r.$$

$\tilde{\gamma}_0 = \gamma_0$ et $\tilde{\gamma}_1 = \gamma_1$. De plus, $H$ étant continue sur un compact, le théorème de Heine nous donne l'existence de $\delta > 0$ tel que

$$|s - s'| < \delta \quad \Longrightarrow \quad \|\gamma_s - \gamma_{s'}\| < r.$$

Si $|s - s'| < \delta$, on a alors $\|\tilde{\gamma}_s - \tilde{\gamma}_{s'}\| < 3r$.
Fixons $s, s' \in [0,1]$ tels que $|s - s'| < \delta$. $\tilde{\gamma}_s$ étant uniformément continu, il existe une subdivision $0 = a_0, a_1, \ldots, a_n = 1$ de $[0,1]$ telle que pour tout $k$, on ait

$$\forall u, v \in [a_k, a_{k+1}], \quad |\tilde{\gamma}_s(u) - \tilde{\gamma}_s(v)| < r.$$

Si $B_k = B(\tilde{\gamma}_s(a_k), 4r)$, on a alors

1. $\forall k$, $B_k \subset \Omega$ (car $|\tilde{\gamma}_s(a_k) - \gamma_s(a_k)| < r$),
2. $\forall k$, $\tilde{\gamma}_s([a_k, a_{k+1}]), \tilde{\gamma}_{s'}([a_k, a_{k+1}]) \subset B_k \cap B_{k+1}$ (car $|\tilde{\gamma}_{s'}(u) - \tilde{\gamma}_s(a_k)| < r + 3r = 4r$).

$f$ étant holomorphe et chaque $B_k$ étant étoilé, elle y admet une primitive $F_k$. De plus, $B_k \cap B_{k-1}$ est connexe donc $F_k - F_{k-1}$ est constant sur $B_k \cap B_{k-1}$. On a donc

$$F_k(\tilde{\gamma}_s(a_k)) - F_{k-1}(\tilde{\gamma}_s(a_k)) = F_k(\tilde{\gamma}_{s'}(a_k)) - F_{k-1}(\tilde{\gamma}_{s'}(a_k))$$

c'est-à-dire

$$\sigma_k := F_k(\tilde{\gamma}_s(a_k)) - F_k(\tilde{\gamma}_{s'}(a_k)) = F_{k-1}(\tilde{\gamma}_s(a_k)) - F_{k-1}(\tilde{\gamma}_{s'}(a_k)).$$

En particulier, $\sigma_0 = \sigma_n = 0$.
On a finalement

$$\sigma$$

$$\begin{aligned}
\int_{\tilde{\gamma}_s} f - \int_{\tilde{\gamma}_{s'}} f &= \sum_{k=1}^{n} \Big( F_k(\tilde{\gamma}_s(a_k)) - F_k(\tilde{\gamma}_s(a_{k-1})) \Big) - \sum_{k=1}^{n} \Big( F_k(\tilde{\gamma}_{s'}(a_k)) - F_k(\tilde{\gamma}_{s'}(a_{k-1})) \Big) \\
&= \sum_{k=1}^{n} \Big( F_k(\tilde{\gamma}_s(a_k)) - F_k(\tilde{\gamma'}_s(a_k)) \Big) - \sum_{k=1}^{n} \Big( F_k(\tilde{\gamma}_s(a_{k-1})) - F_k(\tilde{\gamma}_{s'}(a_{k-1})) \Big) \\
&= \sum_{k=1}^{n} (\sigma_k - \sigma_{k-1}) \\
&= \sigma_n - \sigma_0
\end{aligned}$$

$$= 0.$$

Ainsi,

$$\int_{\tilde{\gamma}_s} f = \int_{\tilde{\gamma}_{s'}} f$$

et en subdivisant l'intervalle $[0,1]$ avec un pas inférieur à $\delta$, on obtient

$$\int_{\gamma_0} f - \int_{\gamma_1} f.$$

Considérons $\Omega = \mathbb{C}^*$. Si $\mathbb{C}^*$ était simplement connexe alors pour tout $f \in \mathscr{H}(\Omega)$ et tout lacet $\gamma$ on aurait

$$\int_{\gamma} f = 0.$$

Or, si $\gamma : t \mapsto e^{2i\pi t}$ et $f = \frac{1}{z}$, on a

$$\int_{\gamma} f = 2i\pi \neq 0$$

donc $\mathbb{C}^*$ n'est pas simplement connexe.

# Nombres de Bell

## Cadre :

On montre que le nombre $B_n$ de partitions de $[\![1,n]\!]$ est donné par

$$B_n = \frac{1}{e}\sum_{n=0}^{+\infty}\frac{k^n}{k!}.$$

**Recasages** :

- 

**Référence** :

## Développement :

Les étapes sont :

1. On montre que $B_{n+1} = \sum_{k=0}^{n}\binom{n}{k}B_k$.
2. On montre que la série $f(z) = \sum_n \frac{B_n}{n!}z^n$ a un rayon de convergence $R \geqslant 1$.
3. On montre que $f(z) = e^{e^z-1}$.
4. On conclut.

1. Une partition de $[\![1,n+1]\!]$ est donnée par un ensemble à $k+1$ éléments contenant $n+1$ ($k$ variant de 0 à $n$, $\binom{n}{k}$ choix par valeur de $k$) et par une partition des $n-k$ éléments restants de $[\![1,n]\!]$ ($B_{n-k}$ choix). Ainsi, on a
$$B_{n+1} = \sum_{k=0}^{n}\binom{n}{k}B_{n-k} = \sum_{k=0}^{n}\binom{n}{n-k}B_k = \sum_{k=0}^{n}\binom{n}{k}B_k.$$
2. Montrons par récurrence forte que $B_n \leqslant n!$. L'inégalité est vraie au rang 0. De plus, si la propriété est vraie jusqu'au rang $n$, on a
$$B_{n+1} = \sum_{k=0}^{n}\binom{n}{k}B_k \leqslant \sum_{k=0}^{n}\binom{n}{k}k! = \sum_{k=0}^{n}\frac{n!}{(n-k)!} \leqslant \sum_{k=0}^{n}n! = (n+1)!.$$
En particulier, la suite $\frac{B_n}{n!}$ est bornée et le rayon de convergence de $f$ est au moins égal à 1.
3. Pour tout $|z|<1$, on a
$$\begin{aligned}
f'(z) &= \sum_{n=1}^{+\infty}\frac{B_n}{(n-1)!}z^{n-1}\\
&= \sum_{n=0}^{+\infty}\frac{B_{n+1}}{n!}z^n\\
&= \sum_{n=0}^{+\infty}\sum_{k=0}^{n}\binom{n}{k}B_k\frac{1}{n!}z^n\\
&= \sum_{n=0}^{+\infty}\sum_{k=0}^{n}\frac{1}{k!(n-k)!}B_k z^n\\
&= \left(\sum_{n=0}^{+\infty}\frac{B_n}{n!}z^n\right)\left(\sum_{n=0}^{+\infty}\frac{1}{n!}z^n\right)\\
&= f(z)e^z.
\end{aligned}$$
Ainsi, il existe $C\in\mathbb{R}$ tel que $f(z) = Ce^{e^z}$. Comme $f(0) = B_0 = 1$, on a $C = e^{-1}$ d'où
$$f(z) = e^{e^z-1}.$$

4. Si $|z| < 1$, on a

$$\begin{aligned} f(z) &= \frac{1}{e} e^{e^z} \\ &= \frac{1}{e} \sum_{n=0}^{+\infty} \frac{e^{zn}}{n!} \\ &= \frac{1}{e} \sum_{n=0}^{+\infty} \sum_{k=0}^{+\infty} \frac{1}{n!} \frac{1}{k!} z^n n^k \\ &= \frac{1}{e} \sum_{k=0}^{+\infty} \frac{1}{k!} \left( \sum_{n=0}^{+\infty} \frac{n^k}{n!} \right) z^k \end{aligned}$$

où la dernière égalité vient du théorème de Fubini. Ainsi, par unicité des coefficients d'un DSE, on a

$$\forall n \in \mathbb{N}, \quad B_n = \frac{1}{e} \sum_{k=0}^{+\infty} \frac{k^n}{k!}.$$

# Méthode de Newton

## Cadre :

Soit $f : [c, d] \to \mathbb{R}$ une fonction de classe $C^2$ avec $f(c)f(d) < 0$ et $f' > 0$. Alors, $f$ admet un unique zéro $a$ et la suite définie par

$$x_{n+1} = F(x_n), \quad F(x) = x - \frac{f(x)}{f'(x)}$$

converge vers $a$ avec une vitesse d'ordre 2 pour $x_0$ suffisamment proche de $a$. Si $f$ est de plus convexe alors pour tout $x_0 \in [c, d]$, la suite $(x_n)_n$ est décroissante ou constante avec

$$0 \leqslant x_{n+1} - a \leqslant C(x_n - a)^2,$$

$$x_{n+1} - a \sim \frac{1}{2}\frac{f''(a)}{f'(a)}(x_n - a)^2.$$

**Recasages** :

- 

**Référence** :

Rouvière

## Développement :

$f$ étant strictement croissante avec $f(c) < 0$ et $f(d) > 0$, le TVI nous assure l'existence et l'unicité de $a$.
Si $x \in I := [c, d]$, la formule de Taylor nous assure l'existence de $z \in [a, x]$ tel que

$$F(x) - a = x - a - \frac{f(x)}{f'(x)} = \frac{f(a) - f(x) - (a - x)f'(x)}{f'(x)} = \frac{1}{2}\frac{f''(z)}{f'(x)}(x - a)^2.$$

Comme $f', f''$ sont continues sur le compact $I$ et que $f' > 0$, on a

$$\inf_{t\in I} f'(t) > 0, \qquad \sup_{t\in I} |f''(t)| < +\infty$$

donc en posant $C = \dfrac{1}{2}\dfrac{\sup_{t\in I}|f''(t)|}{\inf_{t\in I} f'(t)}$, on a

$$\forall x \in I, \qquad |F(x) - a| \leqslant C|x - a|^2.$$

En particulier, si $\alpha > 0$ est tel que $\alpha C < 1$ et $[a + \alpha, a - \alpha] \subset I$, on a

$$|x - a| \leqslant \alpha \implies |F(x) - a| \leqslant C|x - a|^2 \leqslant C\alpha^2 \leqslant \alpha$$

donc $[a + \alpha, a - \alpha]$ est stable par $F$.
Fixons $x_0 \in [a + \alpha, a - \alpha]$. On a donc

$$|x_{n+1} - a| = |F(x_n) - a| \leqslant C|x_n - a|^2.$$

Montrons par récurrence que

$$|x_n - a| \leqslant C^{-1}(C|x_0 - a|)^{2^n}.$$

**Initialisation :** C'est une tautologie pour $n = 0$.

**Hérédité :** Soit $n \in \mathbb{N}$ tel que

$$|x_n - a| \leqslant C^{-1}(C|x_0 - a|)^{2^n}.$$

On a alors

$$|x_{n+1} - a| = |F(x_n) - a| \leqslant C|x_n - a|^2 \leqslant C\Big(C^{-1}(C|x_0 - a|)^{2^n}\Big)^2 = C^{-1}(C|x_0 - a|)^{2^{n+1}}.$$

En particulier, on en déduit que

$$|x_n - a| \leqslant C^{-1}(C\alpha)^{2^n}$$

et comme $C\alpha < 1$, on a bien $x_n \xrightarrow[n\to+\infty]{} a$.

Supposons maintenant $f$ convexe. Alors, si $x \in [a,d]$, on a

$$F(x) - a = \frac{1}{2}\frac{f''(z)}{f'(x)}(x-a)^2 \geqslant 0$$

d'où $[a,d]$ est stable par $F$. De plus, si $x \in [a,d]$, on a

$$F(x) = x - \frac{f(x)}{f'(x)} \leqslant x$$

avec égalité si et seulement si $x = a$. Ainsi, la suite $(x_n)_n$ est constante ou strictement décroissante à valeurs dans $[a,d]$ donc elle converge vers un point fixe de $F$, c'est-à-dire vers $a$.
La converge est d'ordre 2 comme précédemment mais on a mieux : les $z_n$ dans $[a,x_n]$ vérifiant

$$x_{n+1} - a = \frac{1}{2}\frac{f''(z_n)}{f'(x_n)}(x_n-a)^2$$

convergent vers $a$ par comparaison d'où

$$\frac{f''(z_n)}{f'(x_n)} \xrightarrow[n\to+\infty]{} \frac{f''(a)}{f'(a)}$$

et

$$x_{n+1} - a \sim \frac{1}{2}\frac{f''(a)}{f'(a)}(x_n-a)^2.$$

# Caractérisation des fonctions convexes différentiables

## Cadre :

Soit $f : \Omega \to \mathbb{R}$ différentiable. $f$ est convexe si et seulement si

$$\forall x, y \in \Omega, \quad Df(x)(y-x) \leqslant f(y) - f(x).$$

Si $f$ est deux fois différentiables, $f$ est convexe si et seulement si

$$D^2 f(x) \geqslant 0.$$

On en déduit que si

$$E \in \{f \in C([a,b]) \mid f(a) = \alpha,\ f(b) = \beta\}$$

et si $\varphi = \dfrac{\beta - \alpha}{b-a}(x-a) + \alpha$ alors

$$\inf_{f \in E} \int_a^b \sqrt{1 + f'(x)^2}\mathrm{d}x = \int_a^b \sqrt{1 + \varphi'(x)^2}\mathrm{d}x.$$

**Recasages** :

- 

**Référence** :

Rouvière

## Développement :

Supposons $f$ différentiable et convexe. Fixons $x, y \in \Omega$ et posons $g : t \mapsto f(x + t(y-x))$. On a

$$g'(0) = Df(x)(y-x)$$

et

$$\begin{aligned} \frac{g(t) - g(0)}{t} &= \frac{f(x + t(y-x)) - f(x)}{t} \\ &\leqslant \frac{-tf(x) + tf(y)}{t} \\ &= f(y) - f(x) \end{aligned}$$

d'où

$$Df(x)(y-x) \leqslant f(y) - f(x).$$

Réciproquement, si $x, y \in \Omega$ et $z = tx + (1-t)y$, on a

$$Df(z)(y-z) \leqslant f(y) - f(z)$$

$$Df(z)(x-z) \leqslant f(x) - f(z)$$

donc

$$0 = tDf(z)(x-z) + (1-t)Df(z)(y-z) \leqslant tf(x) + (1-t)f(y) - f(z).$$

Supposons maintenant $f$ deux fois différentiables et convexe. Si $x, y \in \Omega$, on a en notant $h = y - x$ :

$$f(x+th) = f(x) + tDf(x)(h) + \frac{1}{2}t^2 D^2 f(x)(h,h) + o(t^2).$$

Ainsi, la caractérisation précédente donne

$$\frac{1}{2}t^2 D^2 f(x)(h,h) + o(t^2) \geqslant 0$$

donc en passant à la limite on trouve

$$D^2 f(x)(h,h) \geqslant 0.$$

Supposons réciproquement que $D^2f(x) \geqslant 0$ pour tout $x \in \Omega$. Si $x, y \in \Omega$, la formule de Taylor donne $c \in [x, y]$ tel que

$$f(y) = f(x) + Df(x)(y-x) + \frac{1}{2}D^2f(c)(y-x, y-x) \geqslant f(x) + Df(x)(y-x)$$

d'où $Df(x)(y-x) \leqslant f(y) - f(x)$ et $f$ est convexe.

Posons $f : x \mapsto \sqrt{1+x^2}$. Cette application étant convexe, on a

$$\forall x, y \in \Omega, \quad \sqrt{1+x^2} - \sqrt{1+y^2} \geqslant \frac{y}{\sqrt{1+y^2}}(x-y).$$

En particulier, si $g \in E$, on a

$$\begin{aligned}
\int_a^b \sqrt{1+g'(x)^2}\mathrm{d}x - \int_a^b \sqrt{1+\varphi'(x)^2}\mathrm{d}x &= \int_a^b \sqrt{1+g'(x)^2} - \sqrt{1+\varphi'(x)^2}\mathrm{d}x \\
&\geqslant \int_a^b \frac{\varphi'(x)^2}{\sqrt{1+(\varphi(x)')^2}}(g'(x)-\varphi'(x))\mathrm{d}x \\
&= \frac{m^2}{\sqrt{1+m^2}}\int_a^b g'(x) - m\mathrm{d}x \\
&= \frac{m^2}{\sqrt{1+m^2}}(g(b)-g(a)-m(b-a)) \\
&= 0.
\end{aligned}$$

# Isomorphisme entre groupes de Lie

## Cadre :

On a $\mathrm{SO}_o(1,2) \simeq \mathrm{PSL}(2,\mathbb{R})$.

**Recasages** :

- 

**Référence** :

## Développement :

Considérons l'action de $\mathrm{SL}(2,\mathbb{R})$ sur le $\mathbb{R}$-espace vectoriel de dimension 3

$$\mathfrak{sl}(2,\mathbb{R}) = \{X \in \mathrm{M}_2(\mathbb{R}) \mid \mathrm{Tr}\, X = 0\}$$

donnée par

$$\begin{array}{ccc} \mathrm{SL}(2,\mathbb{R}) \times \mathfrak{sl}(2,\mathbb{R}) & \to & \mathfrak{sl}(2,\mathbb{R}) \\ (g, X) & \mapsto & gXg^{-1} \end{array}.$$

Cette action est bien définie car la trace est un invariant de similitude et elle laisse invariant le déterminant car c'est également un invariant de similitude :

$$\forall g \in \mathrm{SL}(2,\mathbb{R}), \forall X \in \mathfrak{sl}(2,\mathbb{R}), \quad \det g \cdot X = \det X.$$

Notons $\rho : \mathrm{SL}(2,\mathbb{R}) \to \mathrm{Hom}(\mathfrak{sl}(2,\mathbb{R}))$ le morphisme associé à cette action. Remarquons que si $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \in \mathfrak{sl}(2,\mathbb{R})$, on a

$$\det A = -a^2 - bc = -a^2 - \frac{1}{4}(b+c)^2 + \frac{1}{4}(b-c)^2$$

donc det est une forme quadratique réelle de signature $(1,2)$ sur $\mathfrak{sl}(2,\mathbb{C})$ et $\rho$ envoie $\mathrm{SL}(2,\mathbb{R})$ dans $\mathrm{O}(\mathfrak{sl}(2,\mathbb{R}), \det)$. Le morphisme $\rho$ étant continu (donné dans une base par des fonctions polynomiales) et $\mathrm{SL}(2,\mathbb{R})$ étant connexe, $\mathrm{Im}(\rho)$ contenu dans la composante connexe de $\rho(I_2) = \mathrm{id}_{\mathfrak{sl}(2,\mathbb{R})}$ de $\mathrm{O}(\mathfrak{sl}(2,\mathbb{R}), \det)$. Montrons qu'une fois co-restreinte à cet ensemble, $\rho$ est surjectif. Nous allons pour cela montrer que $\mathrm{Im}(\rho)$ est un ouvert fermé de $\mathrm{O}(\mathfrak{sl}(2,\mathbb{R}), \det)$.

— L'action $\rho$ est en fait la restriction de l'action par similitude

$$\mathrm{GL}(2,\mathbb{R}) \times \mathrm{M}_2(\mathbb{R}) \to \mathrm{M}_2(\mathbb{R})$$

donc elle est lisse. On a de plus

$$\begin{aligned} \rho(I+X) &= \Big(Y \mapsto (I_2+X)Y(I+X)^{-1}\Big) \\ &= \Big(Y \mapsto (I_2+X)Y(I_2-X+o(X))\Big) \\ &= \Big(Y \mapsto Y + XY - YX + o(X)\Big) \\ &= \mathrm{id} + \mathrm{ad}(X) + o(X) \end{aligned}$$

d'où $D\rho(X) = \mathrm{ad}(X)_{|\mathfrak{sl}(2,\mathbb{R})}$. Si $X \in \ker D\rho$, $X$ commute avec

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

donc $X$ est diagonale et est scalaire car $X$ commute avec

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Ainsi, $\rho$ est une immersion en $I_2$ et comme ces sous-variétés ont la même dimension, c'est un difféomorphisme local en $I_2$. De plus, on a

$$\rho \circ L_g = \Big(h \mapsto \rho(gh)\Big) = \Big(h \mapsto \rho(g) \circ \rho(h)\Big) = L_{\rho(g)} \circ \rho$$

d'où

$$D\rho(g) \circ D\mathrm{L}_g(I_2) = D(L_{\rho(g)})(\mathrm{id}_{\mathfrak{sl}(2,\mathbb{R})}) \circ D\rho(I_2)$$

donc $\rho$ est un difféomorphisme local en tout point et est donc ouverte.

— D'après ce qui précède $\mathrm{Im}(\rho)$ est un sous-groupe ouvert de $\mathrm{SO}_o(\mathfrak{sl}(2,\mathbb{R}),\det)$. Ainsi,

$$\mathrm{SO}_o(\mathfrak{sl}(2,\mathbb{R}),\det)\setminus \mathrm{Im}(\rho) = \bigcup_{g\notin \mathrm{Im}(\rho)} g\,\mathrm{Im}(\rho)$$

est un ouvert de $\mathrm{SO}_o(\mathfrak{sl}(2,\mathbb{R}),\det)$ et $\mathrm{Im}(\phi)$ est fermé dans $\mathrm{SO}_o(\mathfrak{sl}(2,\mathbb{R}),\det)$.

Finalement, $\mathrm{Im}(\rho)$ est un ouvert fermé non vide de $\mathrm{SO}_o(\mathfrak{sl}(2,\mathbb{R}),\det)$ donc $\mathrm{Im}(\rho) = \mathrm{SO}_o(\mathfrak{sl}(2,\mathbb{R}),\det)$. Enfin,

$$\ker(\rho) = \{g\in \mathrm{SL}(2,\mathbb{R}) \mid \forall X\in \mathfrak{sl}(2,\mathbb{R}),\ gX = Xg\} = \mathrm{SL}(2,\mathbb{R})\cap(\mathbb{R}I_2) = \{\pm I_2\}.$$

Ainsi, $\rho$ induit l'isomorphisme

$$\mathrm{PSL}(2,\mathbb{R}) \simeq \mathrm{SO}_o(\mathfrak{sl}(2,\mathbb{R}),\det) \simeq \mathrm{SO}_o(1,2).$$

# Projection sur un convexe fermé

## Cadre :

Soit $H$ un espace de Hilbert, $C \subset H$ un convexe fermé et $y \in H$. Il existe un unique $z \in C$ tel que

$$d(y,z) = d(y,C).$$

De plus, $z$ est caractérisé parmi les éléments de $C$ par la propriété :

$$\forall x \in C, \quad \mathrm{Re}\langle y-z, x-z\rangle \leqslant 0.$$

Dans le cas ou $C$ est un sous-espace vectoriel de $H$, la caractérisation devient

$$\forall x \in C, \quad \mathrm{Re}\langle y-z, x-z\rangle \leqslant 0$$

et on en déduit que

$$H = F \oplus F^{\perp}$$

ainsi que le théorème de représentation de Riesz.

**Recasages** :

- 

**Référence** :

## Développement :

On rappelle l'identité du parallélogramme :

$$\forall u, v \in H, \quad \|u+v\|^2 + \|u-v\|^2 = 2\Big(\|u\|^2 + \|v\|^2\Big).$$

Soit $(z_n)_{n\in\mathbb{N}}$ une suite de $C$ telle que

$$d(y,z_n) \xrightarrow[n\to+\infty]{} d(y,C).$$

Pour tous $n, m$, on a

$$\|2y - (z_n+z_m)\|^2 + \|z_n - z_m\|^2 = 2\Big(\|y-z_n\|^2 + \|y-z_m\|^2\Big)$$

d'où

$$\|z_n - z_m\|^2 = 2\Big(\|y-z_n\|^2 + \|y-z_m\|^2\Big) - 4\left\|y - \frac{1}{2}(z_n+z_m)\right\|^2.$$

En particulier, si $\varepsilon > 0$ et si $N \in \mathbb{N}$ est tel que

$$\forall p \geqslant N, \quad |d(y,z_p)^2 - d(y,C)^2| \leqslant \varepsilon$$

alors pour tous $n, m \geqslant N$, on a

$$d(z_n,z_m)^2 \leqslant 2d(y,z_n)^2 + 2d(y,z_m)^2 - 4d(y,C)^2 \leqslant 2\varepsilon.$$

Ainsi, la suite $(z_n)_n$ est de Cauchy et comme $C$ est complet (fermé d'un complet), elle converge vers un élément $z \in C$. Soit $z'$ un autre élément de $C$ vérifiant

$$d(y,z') = d(y,C).$$

Alors, on a

$$\|z-z'\|^2 = 2\Big(\|y-z\|^2 + \|y-z'\|^2\Big) - 4\left\|y - \frac{1}{2}(z+z')\right\|^2 \leqslant 0$$

d'où $z = z'$.

Soit $x \in C$. Pour tout $t \in ]0,1]$, on a

$$\|y - z - t(x-z)\|^2 \geqslant \|y-z\|^2$$

donc

$$\|y-z\|^2 + t^2\|x-z\|^2 - 2t\,\mathrm{Re}\langle y-z, x-z\rangle \geqslant \|y-z\|^2.$$

En particulier

$$t\|x-z\|^2 - 2\,\mathrm{Re}\langle y-z, x-z\rangle \geqslant 0$$

d'où en faisant tendre $t$ vers 0 :

$$\mathrm{Re}\langle y-z, x-z\rangle \leqslant 0.$$

Réciproquement, fixons $z' \in C$ vérifiant

$$\forall x \in C, \quad \mathrm{Re}\langle y-z', x-z'\rangle \leqslant 0.$$

On a alors

$$\begin{aligned}
\|z-z'\|^2 &= \|z-y+y-z'\|^2 \\
&\leqslant \|z-y\|^2 + \|y-z'\|^2 + 2\,\mathrm{Re}\langle z-y, y-z'\rangle \\
&= -\|z-y\|^2 + \|y-z'\|^2 + 2\,\mathrm{Re}\langle y-z, z'-z\rangle \\
&\leqslant -\|z-y\|^2 + \|y-z'\|^2
\end{aligned}$$

# Inégalité de Hoeffding

## Cadre :

Soit $(X_n)_n$ une suite de variables aléatoires indépendantes centrées telle qu'il existe une suite $(c_n)_n \in \mathbb{R}_+^{\mathbb{N}}$ vérifiant

$$|X_n| \leqslant c_n.$$

Alors, pour tout $\varepsilon > 0$, on a

$$\mathbb{P}(|S_n| \geqslant \varepsilon) \leqslant 2\exp\left(-\frac{\varepsilon^2}{2\sum_{k=1}^{n} c_k^2}\right).$$

On en déduit que s'il existe $\alpha, \beta \in \mathbb{R}_+^*$ tels que

$$\sum_{k=1}^{n} c_k^2 \leqslant n^{2\alpha-\beta}$$

alors

$$\frac{S_n}{n^\alpha} \xrightarrow[n\to+\infty]{p.s.} 0.$$

**Recasages** :

- 

**Référence** :

Bernis

## Développement :

Montrons que si $|X| \leqslant 1$ est centrée alors

$$L_X(t) \leqslant e^{\frac{1}{2}t^2}.$$

Si $t \in \mathbb{R}$ et $x \in [-1, 1]$, on a

$$tx = \frac{1-x}{2}(-t) + \frac{1+x}{2}t$$

donc par convexité de l'exponentielle :

$$e^{tx} \leqslant \frac{1-x}{2}e^{-t} + \frac{1+x}{2}e^{t}.$$

Ainsi,

$$\begin{aligned} L_X(t) &= \mathbb{E}(e^{tX}) \\ &\leqslant \mathbb{E}\Big(\frac{1-X}{2}e^{-t} + \frac{1+X}{2}e^{t}\Big) \\ &= \cosh(t). \end{aligned}$$

Or, on a

$$\cosh(t) = \sum_{n=0}^{+\infty} \frac{1}{(2n)!}t^{2n} \leqslant \sum_{n=0}^{+\infty} \frac{1}{2^n n!}t^{2n} = e^{\frac{t^2}{2}}$$

ce qui donne l'inégalité
Obtenons une première inégalité. Par hypothèse, chaque $\frac{X_i}{c_i}$ est sous-gaussienne donc pour tout $t \in \mathbb{R}_+$ et $\varepsilon > 0$, on a

$$\begin{aligned} \mathbb{P}(S_n \geqslant \varepsilon) &= \mathbb{P}(e^{tS_n} \geqslant e^{t\varepsilon}) \\ &\leqslant e^{-t\varepsilon}\mathbb{E}(e^{tS_n}) \\ &= e^{-t\varepsilon}\prod_{k=1}^{n}\mathbb{E}(e^{tX_n}) \end{aligned}$$

$$
\begin{aligned}
&= e^{-t\varepsilon} \prod_{k=1}^{n} \mathbb{E}(e^{tc_k \frac{X_n}{c_k}}) \\
&\leqslant e^{-t\varepsilon} \prod_{k=1}^{n} e^{\frac{t^2 c_k^2}{2}} \\
&= \exp\Big(\frac{t^2}{2} \sum_{k=1}^{n} c_k^2 - t\varepsilon\Big).
\end{aligned}
$$

On cherche alors la meilleure valeur de $t$ pour optimiser cette inégalité. L'exponentielle étant croissante et le trinôme du second degré

$$
\frac{t^2}{2} \sum_{k=1}^{n} c_k^2 - t\varepsilon
$$

atteignant son minimum en

$$
t = \frac{\varepsilon}{\sum_{k=1}^{n} c_k^2},
$$

on obtient l'inégalité

$$
\mathbb{P}(S_n \geqslant \varepsilon) \leqslant \exp\left(-\frac{\varepsilon^2}{2\sum_{k=1}^{n} c_k^2}\right).
$$

En appliquant le même raisonnement à $(-X_k)_k$, on obtient

$$
\mathbb{P}(-S_n \geqslant \varepsilon) \leqslant \exp\left(-\frac{\varepsilon^2}{2\sum_{k=1}^{n} c_k^2}\right)
$$

d'où

$$
\mathbb{P}(|S_n| \geqslant \varepsilon) = \mathbb{P}(S_n \geqslant \varepsilon) + \mathbb{P}(-S_n \geqslant \varepsilon) \leqslant 2\exp\left(-\frac{\varepsilon^2}{2\sum_{k=1}^{n} c_k^2}\right).
$$

Fixons de tels $\alpha, \in \beta\mathbb{R}_+^*$. D'après l'inégalité de Hoeffding, on a pour tout $\varepsilon > 0$ :

$$
\mathbb{P}(|S_n| \geqslant n^\alpha \varepsilon) \leqslant 2\exp\left(-\frac{\varepsilon^2 n^{2\alpha}}{2\sum_{k=1}^{n} c_k^2}\right) \leqslant 2\exp\left(-\frac{\varepsilon^2}{2} n^\beta\right) = o(n^{-2})
$$

donc la série

$$
\sum_{n=0}^{+\infty} \mathbb{P}(|S_n| \geqslant n^\alpha \varepsilon)
$$

converge et d'après le lemme de Borel-Cantelli, on a

$$
\mathbb{P}\left(\limsup_n \left\{\omega \in \Omega \mid \left|\frac{S_n(\omega)}{n^\alpha}\right| \geqslant \varepsilon\right\}\right) = 0.
$$

Pour tout $\varepsilon \in \mathbb{Q}_+^*$, posons

$$
A_\varepsilon = \limsup_n \left\{\omega \in \Omega \mid \left|\frac{S_n(\omega)}{n^\alpha}\right| \geqslant \varepsilon\right\}.
$$

Si $\omega \in A_\varepsilon$, on a

$$
\forall n \in \mathbb{N}, \exists k \geqslant n, \quad \left|\frac{S_n}{n^\alpha}\right| \geqslant \varepsilon
$$

donc

$$
\bigcup_{\varepsilon \in \mathbb{Q}_+^*} A_\varepsilon = \left\{\omega \in \Omega \mid \frac{S_n(\omega)}{n^\alpha} \xrightarrow[n\to+\infty]{\not\longrightarrow} 0\right\}
$$

et comme

$$
\mathbb{P}\left(\bigcup_{\varepsilon \in \mathbb{Q}_+^*} A_\varepsilon\right) \leqslant \sum_{\varepsilon \in \mathbb{Q}_+^*} \mathbb{P}(A_\varepsilon) = 0,
$$

cela implique que

$$
\frac{S_n}{n^\alpha} \xrightarrow[n\to+\infty]{p.s.} 0.
$$

# Intégrale de Fresnel

## Cadre :

On montre que $\displaystyle\int_{\mathbb{R}} \sin(x^2)\mathrm{d}x = \int_{\mathbb{R}} \cos(x^2)\mathrm{d}x = \sqrt{\frac{\pi}{2}}$.

**Recasages** :

- 

**Référence** :

## Développement :

Montrons que les intégrales généralisées

$$\int_{\mathbb{R}_+^*} \frac{e^{ix}}{\sqrt{x}}\mathrm{d}x, \quad \int_{\mathbb{R}} e^{2i\pi x^2}\mathrm{d}x$$

convergent. Pour la première, on remarque que l'intégrande est continue sur $\mathbb{R}_+^*$ et équivalente à $\frac{1}{\sqrt{x}}$ en 0 est y est donc intégrable. De plus, si $A > 0$, on a

$$\int_1^A \frac{e^{ix}}{\sqrt{x}} = \left[\frac{-ie^{ix}}{\sqrt{x}}\right]_1^A - \frac{i}{2}\int_1^A \frac{e^{ix}}{\sqrt{x}^3}\mathrm{d}x$$

et cette quantité admet une limite lorsque $A \to +\infty$ par comparaison à une intégrale de Riemann. Pour la deuxième intégrale, on remarque que si $A > 0$, on a

$$\int_0^A e^{2i\pi x^2}\mathrm{d}x = \frac{1}{2\sqrt{2\pi}}\int_0^{\sqrt{\frac{A}{2\pi}}} \frac{e^{ix}}{\sqrt{x}}\mathrm{d}x$$

donc cette intégrale a la même nature que la première intégrale : elle converge.

Considérons la fonction 1-périodique $f : \mathbb{R} \to \mathbb{C}$ définie par

$$\forall t \in [0,1], \quad f(x) = e^{2i\pi x^2}.$$

$f$ est 1-périodique, continue et $C^1$ par morceaux puisque

$$\lim_{x\to 0^+} e^{2i\pi x^2} = \lim_{x\to 1^-} e^{2i\pi x^2}.$$

Par le théorème de Dirichlet, la série de Fourier de $f$ converge simplement vers $f$. Calculons ses coefficients de Fourier. Si $n \in \mathbb{N}^*$, on a

$$\begin{aligned} c_n(f) &= \int_0^1 e^{2i\pi x^2} e^{-2i\pi nx}\mathrm{d}x \\ &= \int_0^1 e^{2i\pi(x^2-nx)}\mathrm{d}x \\ &= e^{-i\pi\frac{n^2}{2}}\int_0^1 e^{2i\pi(x-\frac{n}{2})^2}\mathrm{d}x \\ &= e^{-i\pi\frac{n^2}{2}}\int_{\frac{n}{2}}^{\frac{n}{2}+1} e^{2i\pi x^2}\mathrm{d}x. \end{aligned}$$

Comme les intégrales étudiées précédemment convergent, la série $\sum_{k\in 2\mathbb{Z}} c_{2k}(f)$ converge et

$$\sum_{k\in 2\mathbb{Z}} c_{2k}(f) = \int_{\mathbb{R}} e^{2i\pi x^2}\mathrm{d}x.$$

De plus, la convergence simple de la série de Fourier de $f$ vers $f$ donne

$$\forall x \in \mathbb{R}, \quad f(x) = \sum_{k\in\mathbb{Z}} c_k(f)e^{2ik\pi}.$$

En particulier, en prenant $x = 0$ et $x = 1$, on obtient

$$f(0) = \sum_{n\in\mathbb{Z}} c_n(f), \quad f(\frac{1}{2}) \sum_{n\in\mathbb{Z}} (-1)^n c_n(f)$$

d'où

$$\int_{\mathbb{R}} e^{2i\pi x^2} \mathrm{d}x = \frac{f(0) + f(\frac{1}{2})}{2} = \frac{1+i}{2}.$$

En identifiant les parties réelles et imaginaires, on obtient la convergence des intégrales

$$\int_{\mathbb{R}} \sin\big(2\pi x^2\big)\mathrm{d}x, \quad \int_{\mathbb{R}} \cos\big(2\pi x^2\big)\mathrm{d}x$$

ainsi que leur valeur. En effectuant le changement de variable $u = \sqrt{2\pi x}$, on obtient alors

$$\int_{\mathbb{R}} \sin\big(x^2\big)\mathrm{d}x = \int_{\mathbb{R}} \cos\big(x^2\big)\mathrm{d}x = \sqrt{\frac{\pi}{2}}.$$

# Injectivité de la transformée de Fourier sur $L^1(\mathbb{R})$.

## Cadre :

On démontre que si $\gamma_a(x) = e^{-ax^2}$ alors $\hat{\gamma}_a(x) = \sqrt{\frac{\pi}{a}}\gamma_{\frac{\pi^2}{a^2}}$.

On en déduit que si $f \in L^1(\mathbb{R})$ vérifie $\hat{f} = 0$ alors $f = 0$ presque partout.

**Recasages** :

- 

**Référence** :

El Amrani

## Développement :

Remarquons tout d'abord que $\gamma_a$ est continue et $\gamma_a = o(x^{-2})$ en $\pm\infty$ et est donc intégrable. Fixons $\xi \in \mathbb{R}$. On a

$$\hat{\gamma}_a(\xi) = \int_{\mathbb{R}} e^{-2i\pi x\xi} e^{-ax^2} \mathrm{d}x = \int_{\mathbb{R}} e^{-a(x^2 + \frac{2}{a} i\pi\xi x)} \mathrm{d}x = e^{-\frac{\pi^2}{a^2}\xi^2} \int_{\mathbb{R}} e^{-a(x+\frac{1}{a}i\pi\xi)^2} \mathrm{d}x.$$

Pour $R > 0$, considérons le contour

$$\Gamma = \Gamma_1 \wedge \Gamma_2 \wedge \Gamma_3 \wedge \Gamma_4 = [-R, R] \wedge [R, R + i\frac{\pi}{a}\xi] \wedge [R + i\frac{\pi}{a}\xi, -R + i\frac{\pi}{a}\xi] \wedge [-R + i\frac{\pi}{a}\xi, -R].$$

$\gamma_a$ étant intégrable sur $\mathbb{R}$, on a

$$\int_{\Gamma_1} \gamma_a \xrightarrow[R\to+\infty]{} \int_{\mathbb{R}} e^{-ax^2} \mathrm{d}x = \sqrt{\frac{\pi}{a}}.$$

De même, l'intégrale définissant $\hat{\gamma}_a(\xi)$ étant absolument convergente, on a

$$\int_{\Gamma_3} \gamma_a \xrightarrow[R\to+\infty]{} -\int_{\mathbb{R}} e^{-a(x+i\frac{\pi}{a}\xi)^2} \mathrm{d}x.$$

Étudions l'intégrale de $\gamma_a$ sur $\Gamma_2$. On a

$$\begin{aligned}
\left|\int_{\Gamma_2} \gamma\right| &= \left| i \int_0^{\frac{\pi}{a}\xi} e^{-a(R+it)^2} \mathrm{d}t \right| \\
&\leqslant e^{-\frac{R^2}{2}} \int_{min(0,\frac{\pi}{a}\xi)}^{\max(0,\frac{\pi}{a}\xi)} e^{at^2} \mathrm{d}t \\
&\xrightarrow[R\to+\infty]{} 0.
\end{aligned}$$

De même,

$$\int_{\Gamma_4} \gamma_a \xrightarrow[R\to+\infty]{} 0.$$

Or, le théorème de Cauchy sur un convexe donne

$$\int_{\Gamma} \gamma_a = 0$$

donc en passant à la limite dans cette égalité, on trouve

$$\hat{\gamma}_a(\xi) = \sqrt{\frac{\pi}{a}} e^{-\frac{\pi^2}{a^2}\xi^2} = \sqrt{\frac{\pi}{a}} \gamma_{\frac{\pi^2}{a^2}}(\xi).$$

Fixons $f \in L^1(\mathbb{R})$ vérifiant $\hat{f} = 0$. Si $a > 0$ et $z \in \mathbb{R}$, on a alors :

$$\begin{aligned}
0 &= \int_{\mathbb{R}} \hat{f}(\xi) e^{iz\xi} \gamma_a(\xi) \mathrm{d}\xi \\
&= \int_{\mathbb{R}} f(\xi) \hat{\gamma}_a(z - \xi) \mathrm{d}\xi \\
&= f * \hat{\gamma}(z).
\end{aligned}$$

Puisque $\hat{\gamma}_a = \sqrt{\frac{\pi}{a}}\gamma_1\left(\sqrt{\frac{\pi}{a}}\right)$, $(\hat{\gamma}_a)_{a>0}$ est une approximation de l'identité, on a alors

$$f = \lim_{a\to 0} f * \hat{\gamma} = \lim_{a\to 0} 0 = 0$$

donc la transformation de Fourier est injective.

# Forme normale de Smith

## Cadre :

Si $A$ est un anneau euclidien, pour toute matrice $M \in M_{n,m}(A)$, il existe d'unique éléments $f_1, \dots, f_r \in A$ (à association près) tels $M$ soit équivalente à

$$\begin{pmatrix} f_1 & & & & & \\ & \ddots & & & & \\ & & f_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

avec $f_1 \mid \cdots \mid f_r$.

**Recasages** :

- 

**Référence** :

## Développement :

Si $M$ est nulle, il n'y a rien à faire. On suppose donc $M$ non nulle.
**Existence :** Soit $f_1 \in A$ un élément non nul de stathme minimal parmi les coefficients des matrices équivalentes à $M$ et soit $U$ une matrice équivalente à $M$ ayant $f_1$ en haut à gauche. Considérons un coefficient $b$ sur la première ligne ou colonne de $A$ et posons $b = aq + r$ une division euclidienne de $b$ par $a$. Supposons que $r \neq 0$. Alors, en effectuant une opération élémentaire sur les colonnes ou les lignes pour soustraire $aq$ à $b$, on trouve un coefficient non nul d'une matrice équivalente à $M$ ayant un stathme strictement inférieur à $a$, ce qui est absurde. Ainsi, $r = 0$ et on peut effectuer une opération élémentaire sur les colonnes ou les lignes pour transformer le coefficient $b$ en 0. Ainsi, $M$ est équivalente à une matrice de la forme

$$\begin{pmatrix} f_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & M' & \\ 0 & & & \end{pmatrix}.$$

Si $c$ est un coefficient de $M'$ alors en ajoutant la première ligne à la ligne contenant $c$ puis en effectuant une opération sur les colonnes, on peut de même remplacer $c$ par son reste dans la division euclidienne par $a$. Par minimalité de $N(a)$, ce reste doit être nul et $c$ est donc divisible par $a$. Ainsi, $M$ est équivalente à une matrice de la forme

$$\begin{pmatrix} f_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & f_1 M'' & \\ 0 & & & \end{pmatrix}.$$

On obtient alors l'existence de la décomposition par récurrence sur la taille de $M$.

**Unicité :** Fixons $k \leqslant \min(n, m)$ et posons $I_k(M)$ l'idéal engendré par les mineurs de taille $k$ de $M$. Appliquer une opération élémentaire à $M$ remplace ses mineurs de taille $k$ par une combinaison $A$-linéaire des mineurs de taille $k$ de $M$ donc

$$\forall P, Q \in \mathrm{GL}(n, A), \quad I_k(PMQ) \subset I_k(M).$$

Puisque

$$M = P^{-1}(PMQ)Q^{-1},$$

en en déduit que

$$\forall P, Q \in \mathrm{GL}(n, A), \quad I_k(PMQ) = I_k(M).$$

Ainsi, si deux familles $f_1, \dots, f_r, f'_1, \dots, f'_s \in A$ vérifiant les propriétés du théorème existent, on a $r = \operatorname{rang} M = s$ et pour tout $k \in [\![1, s]\!]$, on a

$$\langle f_1 \cdots f_k \rangle = \langle f'_1 \cdots f'_k \rangle$$

. En particulier, il existe $u_k \in A^\times$ tel que

$$f_1 \cdots f_k = f'_1 \cdots f'_k$$

et en utilisant l'intégrité de $A$ pour simplifier au fur et à mesure, on trouve

$$f_1 \sim f'_1, \ldots, f_s \sim f'_s$$

d'où l'unicité.

# Critère de cyclicité de $\mathbb{Z}/n\mathbb{Z}^*$

## Cadre :

$\mathbb{Z}/n\mathbb{Z}^*$ est cyclique si et seulement si $n = 2, 4$ ou $n = p^\alpha, 2p^\alpha$ avec $p \in \mathbb{P}$ et $\alpha \in \mathbb{N}^*$.

**Recasages** :

- 

**Référence** :

## Développement :

On commence par montrer que si $n_1, n_2 \in \mathbb{N}^*$ vérifient $n_1 \wedge n_2 = 1$ et $\varphi(n_1) \wedge \varphi(n_2) \neq 1$ alors $\mathbb{Z}/n_1n_2\mathbb{Z}$ n'est pas cyclique.
Fixons de tels entiers. Par le théorème chinois, on a

$$\mathbb{Z}/n_1n_2\mathbb{Z}^* \simeq \mathbb{Z}/n_1\mathbb{Z}^* \times \mathbb{Z}/n_2\mathbb{Z}^*.$$

Si $(a, b) \in \mathbb{Z}/n_1\mathbb{Z}^* \times \mathbb{Z}/n_2\mathbb{Z}^*$, on a

$$(a, b)^{\varphi(n_1)\vee\varphi(n_2)} = (1, 1)$$

donc

$$\operatorname{ord}(a, b) \leqslant \varphi(n_1) \vee \varphi(n_2) = \frac{\varphi(n_1)\varphi(n_2)}{\varphi(n_1) \wedge \varphi(n_2)} < \varphi(n_1)\varphi(n_2) = |\mathbb{Z}/n_1\mathbb{Z}^* \times \mathbb{Z}/n_2\mathbb{Z}^*|.$$

En particulier, aucun élément de $\mathbb{Z}/n_1\mathbb{Z}^* \times \mathbb{Z}/n_2\mathbb{Z}^*$ n'est un générateur et $\mathbb{Z}/n_1n_2\mathbb{Z})^*$ n'est pas cyclique.

Montrons maintenant par récurrence que pour tout $k \in \mathbb{N}$, il existe $\lambda \in \mathbb{N}$ tel que

$$\begin{cases} (1 + p)^{p^k} = 1 + \lambda_k p^{k+1}, \\ \lambda_k \wedge p = 1. \end{cases}$$

**Initialisation :** Pour $k = 0$, $\lambda_0 = 1$ convient.

**Hérédité :** Soit $k \in \mathbb{N}$ tel qu'il existe un tel $\lambda_k \in \mathbb{N}^*$. On a alors

$$\begin{aligned} (1 + p)^{p^{k+1}} &= (1 + \lambda_k p^{k+1})^p \\ &= \sum_{j=0}^{p} \binom{p}{j} \lambda_k^j p^{(k+1)j} \\ &= 1 + \sum_{j=1}^{p-1} \binom{p}{j} \lambda_k^j p^{(k+1)j} + \lambda_k^p p^{(k+1)p}. \end{aligned}$$

Comme $p \mid \binom{p}{k}$ pour $k = 1, \ldots, p - 1$, le nombre

$$\lambda_{k+1} = \frac{1}{p^{k+2}} \left( \sum_{j=1}^{p-1} \binom{p}{j} \lambda_k^j p^{(k+1)j} + \lambda_k^p p^{(k+1)p} \right) \in \mathbb{N}$$

convient puisqu'il congrue à $\lambda_k$ modulo $p$.

Démontrons le théorème. Fixons $n \in \mathbb{N}^*$ et posons

$$n = 2^m \prod_{k=1}^{s} p_k^{\alpha_k}$$

sa décomposition en facteurs premiers. On distingue plusieurs cas.

— Si $s = 0$ et $m \in \{0, 1, 2\}$, $\mathbb{Z}/n\mathbb{Z}^*$ est de cardinal 1 ou 2 donc est cyclique.

— Si $s = 0$ et $m > 3$, $\mathbb{Z}/n\mathbb{Z}^*$ se surjecte sur $\mathbb{Z}/8\mathbb{Z}^*$. Or, tous les éléments de $\mathbb{Z}/8\mathbb{Z}^* = \{1, 3, 5, 7\}$ sont d'ordre 2 donc $\mathbb{Z}/8\mathbb{Z}^*$ n'est pas cyclique et $\mathbb{Z}/n\mathbb{Z}^*$ non plus.

— Si $s > 1$ alors en posant $n_1 = p_1^{\alpha_1}$ et $n_2 = \frac{n}{n_1}$, on a

$$\begin{cases} n = n_1 n_2, \\ n_1 \wedge n_2 = 1, \\ 2 \mid \varphi(n_1), \varphi(n_2) \end{cases}$$

donc le premier lemme implique que $\mathbb{Z}/n\mathbb{Z}^*$ n'est pas cyclique.

— Si $s = 1$ et $m12$, on a $n = 2^m p_1^{\alpha_1}$ et le premier lemme permet d'affirmer que $\mathbb{Z}/n\mathbb{Z}^*$ n'est pas cyclique.

— Supposons maintenant que $s = 1$ et $m \in \{0, 1\}$. Le théorème chinois donne

$$\mathbb{Z}/n\mathbb{Z}^* \simeq \mathbb{Z}/2^m\mathbb{Z}^* \times \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}^* \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}^*.$$

Montrons que $\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}^*$ est cyclique. D'après notre second lemme, $1 + p_1$ est d'ordre $p_1^{\alpha_1 - 1}$ dans $\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}^*$. De plus, le morphisme $\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}^* \to \mathbb{Z}/p_1\mathbb{Z}^*$ étant surjectif, on peut trouver un élément $x$ dans $\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}^*$ d'ordre $p_1 - 1$. Alors, $(1 + p_1)x$ est d'ordre $(p_1 - 1)p_1^{\alpha_1 - 1} = |\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}^*|$ d'où $\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}^*$ est cyclique.

# $\mathrm{GL}(n,\mathbb{C})$ n'a pas de petits sous-groupes

## Cadre :

Si $G$ est un sous-groupe fermé de $\mathrm{GL}(n,\mathbb{C})$ alors les éléments de $G$ sont diagonalisables et leurs valeurs propres sont de module 1. Si de plus $G \subset B(1,\sqrt{3})$ alors $G = \{I\}$.

**Recasages** :

- 

**Référence** :

Oraux X-ENS, algèbre 2

## Développement :

Soient $C > 0$ tel que $G \subset B(I,C)$ et $A \in G$. Fixons $\lambda \in \mathrm{Sp}(A)$ et $X$ un vecteur propre de $A$ pour $\lambda$. On a

$$|\lambda|\|X\| = \|\lambda X\| = \|AX\| \leqslant \|A\|\|X\|$$

d'où $|\lambda| \leqslant \|A\| \leqslant C$. De plus, si $n \in \mathbb{Z}$, $\lambda^n \in \mathrm{Sp}(A^n)$ et $A^n \in G$ donc $|\lambda^n| \leqslant C$. En particulier, la suite $(\lambda^n)_{n\in\mathbb{Z}}$ est bornée et on a donc $|\lambda| = 1$. Montrons maintenant que $A$ est diagonalisable. Posons $A = D + N$ sa décomposition de Dunford. Raisonnons par l'absurde et supposons que $A$ n'est pas diagonalisable. Alors, l'indice de nilpotence $s$ de $N$ est strictement supérieur à 1 et $\ker N \subsetneq \ker N^2$ donc il existe $X \in \ker N^2 \setminus \ker N$. Si $p \geqslant s$, on a alors

$$A^pX = (D+N)^pX = D^pX + pD^{p-1}NX$$

donc

$$\left\|D^pX + pD^{p-1}NX\right\| \leqslant \|A^pX\| \leqslant \|A^p\|\|X\| \leqslant C\|X\|$$

ce qui est absurde car le membre de gauche n'est pas borné. Ainsi, $A$ est diagonalisable.

Supposons maintenant que $G \subset B(0,\sqrt{2})$ et fixons $A \in G$. Puisque toute matrice de $G$ est diagonalisable, il nous suffit de montrer que les valeurs propres de $A$ sont toutes égales à 1. Fixons donc $\lambda \in \mathrm{Sp}(A)$. On a alors

$$|\lambda - 1| \leqslant \|A - I\| < \sqrt{2}.$$

Puisque $\lambda^n \in \mathrm{Sp}(A^n)$ pour tout $n \in \mathbb{N}$, on a également

$$|\lambda^n - 1| < \sqrt{2}$$

pour tout $n \in \mathbb{N}$. De plus, $\lambda \in S^1$ d'après la première partie donc il existe $\theta \in \mathbb{R}$ tel que $\lambda = e^{i\theta}$. Or, on a

$$\begin{aligned}
|\lambda^n - 1|^2 \leqslant 2 &\iff (cosn\theta - 1)^2 + \sin n\theta \leqslant 2 \\
&\iff 2 - 2\cos n\theta \leqslant 2 \\
&\iff \cos n\theta \geqslant 0 \\
&\iff n\theta \in \left[\frac{-\pi}{2}, \frac{\pi}{2}\right] \pmod{2\pi}
\end{aligned}$$

et cette condition ne peut pas être vérifiée pour tout $n \in \mathbb{N}$ si $\theta \neq 0$ d'où $\lambda = 1$ et $G$ est trivial.

# Extrema liés

## Cadre :

RESULTAT

**Recasages** :

- 

**Référence** :

## Développement :

Soit $M$ une variété, $a \in M$ et $\varphi : U \to \mathbb{R}^k \times \{0\}$ une carte locale. Montrons que $d_a\varphi(T_aM) = \mathbb{R}^k \times \{0\}$. Fixons $v \in T_aM$. Comme $\varphi$ est à valeurs dans $\mathbb{R}^k \times \{0\}$, $d_a\varphi$ est à valeurs dans $T_{\varphi(a)}\Big(\mathbb{R}^k \times \{0\}\Big) = \mathbb{R}^k \times \{0\}$ d'où $v \in \mathbb{R}^k \times \{0\}$.
Réciproquement, fixons $v \in \mathbb{R}^k \times \{0\}$. Pour $t$ suffisamment petit, on a $\varphi(a) + tv \in \varphi(U)$. On peut alors poser

$$\begin{array}{ccc} ]-\delta,\delta[ & \to & U \subset M \\ t & \mapsto & \varphi^{-1}(\varphi(a)+tv) \end{array}$$

et on a

$$v = \frac{\mathrm{d}}{\mathrm{d}t}_{|t=0}(\varphi(a)+tv) = \frac{\mathrm{d}}{\mathrm{d}t}_{|t=0}(\varphi\Big(\varphi^{-1}\Big(\varphi(a)+tv)\Big)\Big) = d_a\varphi\Big(\frac{\mathrm{d}}{\mathrm{d}t}_{|t=0}\varphi^{-1}\Big(\varphi(a)+tv)\Big)\Big) \in d_a\varphi(U).$$

Supposons maintenant que $M = \{x \in \mathbb{R}^n \mid g_1(x) = \cdots = g_{n-k}(x) = 0\}$ et que $(d_ag_1, \ldots, d_ag_{n-k})$ est libre. Posons $T = \bigcap_{j=1}^{n-k} \ker(d_ag_j)$. Alors, $T$ est un espace vectoriel de même dimension que $T_aM$ et de plus, si $v = \gamma'(0) \in T_aM$ alors

$$\forall j, \forall t, \quad g_j \circ \gamma(t) = 0$$

donc en dérivant :

$$\forall j, \quad d_ag_j(v) = 0.$$

Ainsi, $T_aM \subset T$ et $T = T_aM$.

Considérons maintenant $f : M \to \mathbb{R}$ différentiable et atteignant un extremum local en $a \in M$. Posons $\varphi : U \to \mathbb{R}^k$ une carte locale autour de $a$. Alors, $f \circ \varphi^{-1}$ admet un extremum local en $\varphi(a)$ d'où $d_{\varphi(a)}(f \circ \varphi^{-1}) = 0$. Or, on a

$$d_{\varphi(a)}(f \circ \varphi^{-1}) = d_af \circ d_{\varphi(a)}\varphi^{-1} = d_af \circ \Big(d_a\varphi\Big)^{-1}$$

d'où $d_af_{|T_aM} = 0$. En particulier, on a

$$\bigcap_{j=1}^{n-k} \mathrm{Vect}(d_ag_j)^\perp = \bigcap_{j=1}^{n-k} \ker(d_ag) = T_aM \subset \ker(d_af) = \mathrm{Vect}(d_af)^\perp$$

d'où

$$\mathrm{Vect}(d_af) \subset \left(\bigcap_{j=1}^{n-k} \mathrm{Vect}(d_ag_j)^\perp\right)^\perp = \sum_{j=1}^{n-k} \mathrm{Vect}(d_ag)^\perp = \mathrm{Vect}(d_ag_1, \ldots, d_ag_{n-k}).$$

Considérons $u \in L(E)$ un endomorphisme symétrique d'un espace euclidien et $S$ la sphère unité de $E$. L'application $P : x \mapsto \langle u(x), x\rangle$ étant continue sur $S$ et $S$ étant compact, elle y est bornée et atteint y ses bornes. Posons $x \in S$ tel que

$$P(x) = \sup_{y \in S} P(y).$$

Alors, $x$ est un extremum local de $P$ sur $S$. $S$ étant une sous-variété de $E$ décrite par l'équation

$$N(x)^2 = 1$$

qui provient d'une submersion, le théorème des extrema liés assure l'existence de $\lambda \in \mathbb{R}$ tel que

$$d_x P = \lambda d_x N^2.$$

Or,

$$\forall h \in E, \quad d_x P(h) = \langle u(x), h\rangle = \langle u(h), x\rangle = 2\langle u(x), h\rangle$$

et

$$\forall h \in E, \quad d_x N^2(h) = \langle x, h\rangle + \langle h, x\rangle = 2\langle x, h\rangle$$

donc par non dégénérescence du produit scalaire, $u(x) = \lambda x$ et $x$ est un vecteur propre de $u$. Comme $u$ stabilise $\mathrm{Vect}(x)$, il stabilise aussi son orthogonal et on conclut par récurrence sur la dimension de $E$.